NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

**INTERNETWORKING:
TECHNICAL STRATEGY FOR IMPLEMENTING
THE NEXT GENERATION INTERNET PROTOCOL
(IPV6) IN THE MARINE CORPS
TACTICAL DATA NETWORK**

by

James E. Nierle

June 1996

Co-Advisors: Dan Boger
Don Brutzman

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE June, 1996	3. REPORT TYPE AND DATES COVERED Master's Thesis

. TITLE AND SUBTITLE INTERNETWORKING: TECHNICAL STRATEGY FOR IMPLEMENTING THE NEXT GENERATION INTERNET PROTOCOL (IPv6) IN THE MARINE CORPS TACTICAL DATA NETWORK	5. FUNDING NUMBERS
. AUTHOR(S) Nierle, James E.	
. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

1. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

2a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	12b. DISTRIBUTION CODE

3. ABSTRACT *(maximum 200 words)*

The Marine Corps must architect a tactical internet based on a software technology that is in transition - the Internet Protocol (IP). ›evelopment of the Marine Corps' tactical internetworking system (Tactical Data Network or TDN) is progressing concurrently with the lobal Internet community's development of the Next Generation Internet Protocol (IPv6). Current (IPv4) and next generation (IPv6) ersions of the Internet Protocol can together meet the tactical internetworking needs of the Marine Corps.

IPv4 provides universal interoperability with other networking technologies and support for a wide range of services now, but ·ithout enhancements IPv4 cannot meet the long-terms needs of evolving tactical applications. IPv6 is needed to meet emerging equirements (such as secure mobility) but is not yet ready for implementation in the Tactical Data Network. Therefore the Marine Corps iust build the tactical internet architecture using IPv4 and incorporate IPv6 improvements when transition is possible.

Marine Corps commitment to IP is essential to ensure universal interoperability and hardware-independent evolution of tactical pplications and networking technology. This work presents a tactical IP addressing plan for TDN that works with IPv4 and also facilitates nooth transition to IPv6. In concert with the other military services, the Marine Corps must develop a strategy for migrating the joint ictical internet to IPv6. The future viability of the Tactical Data Network depends on the Internet Protocol.

4. SUBJECT TERMS internetworking, Internet, IPv4, IPv6, Next Generation Internet Protocol,Tactical Data Network, U.S. Marine Corps, migration strategy	15. NUMBER OF PAGES 219
	16. PRICE CODE

7. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

INTERNETWORKING:
TECHNICAL STRATEGY FOR IMPLEMENTING THE NEXT GENERATION INTERNET PROTOCOL (IPV6) IN THE MARINE CORPS TACTICAL DATA NETWORK

James E. Nierle
Captain, United States Marine Corps
B.S., University of Southern California, 1985

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
[COMMAND, CONTROL, and COMMUNICATIONS]

from the

NAVAL POSTGRADUATE SCHOOL
June 1996

Author: James E. Nierle

James E. Nierle

Approved by: Dan C Boger

Dan Boger, Co-Advisor

Don Brutzman, Thesis Advisor

Dan C Boger

Dan C. Boger, Chairman
Command Control & Communications (C3) Academic Group

ABSTRACT

The Marine Corps must architect a tactical internet based on a software technology that is in transition - the Internet Protocol (IP). Development of the Marine Corps' tactical internetworking system (Tactical Data Network or TDN) is progressing concurrently with the global Internet community's development of the Next Generation Internet Protocol (IPv6). Current (IPv4) and next generation (IPv6) versions of the Internet Protocol can together meet the tactical internetworking needs of the Marine Corps.

IPv4 provides universal interoperability with other networking technologies and support for a wide range of services now, but without enhancements IPv4 cannot meet the long-terms needs of evolving tactical applications. IPv6 is needed to meet emerging requirements (such as secure mobility) but is not yet ready for implementation in the Tactical Data Network. Therefore the Marine Corps must build the tactical internet architecture using IPv4 and incorporate IPv6 improvements when transition is possible.

Marine Corps commitment to IP is essential to ensure universal interoperability and hardware-independent evolution of tactical applications and networking technology. This work presents a tactical IP addressing plan for TDN that works with IPv4 and also facilitates smooth transition to IPv6. In concert with the other military services, the Marine Corps must develop a strategy for migrating the joint tactical internet to IPv6. The future viability of the Tactical Data Network depends on the Internet Protocol.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The author gratefully acknowledges the financial support of the Tactical Data Network Project Office, C4I Division, Marine Corps Systems Command, in researching this thesis. The author would also like to thank his wife, Jeanne, for her unwavering support throughout this arduous project.

EXECUTIVE SUMMARY

The Marine Corps is experiencing a revolution in tactical information technology. The Corps is fielding a generation of C4I systems that will empower Marines at every tactical echelon to wage information-age warfare. The Tactical Data Network (TDN) weaves these various end-user systems into a tactical internetwork which permits seamless information exchange across the battlespace. The proposed TDN architecture incorporates the Internet Protocol (IP), the same technology underlying the global Internet. IP is itself in a period of transition to a Next Generation Internet Protocol (IPng), formally called Internet Protocol version 6 (IPv6). Marine Corps program planners, network architects, and potential tactical internet users must ensure that IPv6 transition planning is integral to the design and deployment of TDN. Formulation of an IPv6 migration strategy now is essential to ensure the future viability of both TDN and the tactical internet.

The Tactical Data Network is a system of commercial routers, workstations, LAN repeaters and hubs, military encryption devices, and other internetworking equipment and software. TDN interconnects end-user computers via local-area networks (LANs) and interconnects LANs to form a tactical internet. Analysis of evolving Marine Corps tactical end systems and applications reveals that there are five crucial tactical internetworking needs that TDN must fulfill: *addressing, multicasting, mobility, quality of service control,* and *security.* Unique identification (addressing) of every end-system connected to the tactical internet is necessary for universal communication. The method of allocating addresses must be logical, simple, and (ideally) automatic. Tactical military communications is inherently many-to-many multicast. TDN must provide multicast support for simultaneous dissemination of information (such as the Common Operational Picture) and for efficient utilization of limited communications bandwidth. Mobile users of TDN must be free to roam the battlespace and retain seamless access to network services. Emerging tactical applications such as distributed collaborative

planning (DCP) and distributed interactive simulation (DIS) require guaranteed minimum thresholds of bandwidth and latency in order to function across low-bandwidth intermittent tactical communications links. Priority of network resource usage must also be maintained across the TDN infrastructure. Security must be provided for data in transit across the network, and networking devices themselves must be protected from intrusion and/or corruption. Finally, the Marine Corps TDN must fit within the joint tactical internetworking architecture. A robust yet simple internetworking protocol (or set of protocols) is needed within TDN to fulfill these many diverse requirements.

Internet Protocol version 4 (IPv4) is the *de facto* open systems internetworking standard. The simplicity, robustness, and openness of IPv4 have made it enormously popular in the global Internet and in many large private "intranets." Exponential growth of the Internet, the revolution in mobile computing, the advent of real-time, multicast multimedia applications, and the emergence of information warfare and electronic commerce are combining to expose IPv4's limitations. However, enhancements to IPv4 such as *IP Multicast, Mobile IP*, and the *IP Security Architecture* will satisfy most of the Marine Corps' short-term internetworking requirements. Indeed no suitable alternative currently exists. Nevertheless it is unwise to expect IPv4 to meet military internetworking needs into the 21st century.

IPv6 is an *evolutionary* step forward from IPv4, not a *revolutionary* replacement of IPv4. IPv6 retains the fundamental connectionless packet delivery service of IPv4 and also adds new functionality to improve scaleability and to support a broader range of applications. The major improvements of IPv6 over IPv4 include:

- Expansion of the IP address space and a more versatile address hierarchy.
- A new type of addressing called *anycast* that is conceptually a cross between unicast and multicast.
- IP address autoconfiguration that enables "plug and play" connection to the network.
- Native multicast capability (IP Multicast) and an improved mechanism for controlling the scope of multicast sessions.

- A new protocol mechanism for controlling quality of service (QoS).
- Native support for security at the IP (internet) layer.

IPv6 formal structure is defined and it is on track to become an *Internet Standard.* IPv6 will eventually replace IPv4 throughout the global Internet and in most private TCP/IP networks as well. Commercial software products based on IPv6 will be available when TDN is fielded. The Marine Corps' transition to IPv6 will be driven by the quality of service requirements of next generation tactical software applications. The timing of the Corps' migration to IPv6 will be affected by the maturity of IPv6 as well as by the migration plans of the other military services. When the IPv4-to-IPv6 transition does commence, IPv6 must be incrementally deployed in the tactical internet to ensure the availability of IPv6 capabilities and backward compatibility with IPv4-only systems.

The IP addressing plan is a key element of the TDN architecture. The tactical addressing plan proposed in this study is based on successful IPv4 protocols and best current Internet practices that will facilitate a smooth transition to IPv6.

Adoption of IP as the centerpiece of the tactical internet architecture is essential. The Marine Corps gains significant technology leverage by basing its tactical internet on the protocols of the global Internet. The current version of the Internet Protocol (IPv4) is highly stable and mature, widely implemented and well-understood. IPv4 adequately supports the internetworking demands of current tactical data systems and software applications. IPv6's enhanced features are needed to support tactical internetworking in the next century and must be included in the long-term tactical internet architecture. However, basing the design of TDN entirely on IPv6 is not prudent because significant deployment and testing of IPv6 implementations remains to be accomplished. Therefore it is recommended that the TDN design proceed based on the proven capabilities of IPv4 and be influenced by expected IPv6 improvements. A strategy for transitioning to IPv6 must be mapped out now, and an IPv6 upgrade path must be designed into all tactical internet systems in order to avoid costly re-engineering later.

I. INTRODUCTION

A. MOTIVATION

The Marine Corps is experiencing a revolution in tactical information technology. In the next few years the Corps will field a generation of C4I systems that will empower tactical commanders as never before. Internetworking component systems will further leverage new technology by permitting seamless information exchange across the battlespace.

At the core of the tactical internetwork will be a data switching system called Tactical Data Network (TDN). The TDN architecture incorporates the Internet Protocol (IP), the same technology that underlies the global Internet. IP is itself in a period of transition to a Next Generation Internet Protocol (IPng), formally called Internet Protocol version 6 (IPv6). Marine Corps program planners, network architects, and potential tactical internet users must formulate migration strategies now in order to be ready to capitalize on these enormous turn-of-the-century changes.

B. OBJECTIVES

The objective of this study is to identify the major issues that must be addressed as the Marine Corps prepares to field a tactical internet (TDN) based on a technology in transition, namely the Internet Protocol (IP). This work provides specific recommendations for an IP addressing architecture that supports the internetworking requirements of tactical end systems. This work also provides strategic network planning recommendations to facilitate a smooth migration to IPv6.

C. ORGANIZATION OF THE STUDY

This thesis provides Marine Corps decision makers with information regarding the major issues of tactical networking affected by the Internet Protocol (IP). Following analyses of both the current version of IP (IP version 4) and the next generation IP (IP

version 6), Internet Protocol migration strategy considerations are discussed. Finally, recommendations are made for issues needing further study.

Chapter II provides background information regarding the Internet Protocol and describes research efforts related to tactical internetworking and to the development of IPv6. Chapter III presents an overview of the Tactical Data Network (TDN), the environment in which it will operate, and the concept of how it will be employed. Chapter IV identifies the internetworking requirements of the tactical data systems that will employ TDN as their communications backbone. Chapters V and VI contain analysis of how well IPv4 and IPv6 each satisfy the tactical internetworking requirements identified in Chapter IV.

Chapter VII then fuses the information in the first six chapters to produce a recommended addressing architecture for TDN. The detailed IP addressing plan for the Tactical Data Network is contained in Appendix A.

Chapter VIII identifies IPv6 migration options available to the Marine Corps and the key issues that must be considered in developing an IPv6 migration strategy. Chapter IX presents conclusions and recommendations for future work.

II. BACKGROUND AND RELATED WORK

A. INTRODUCTION

Internetworking technology is an enormous field of science and engineering. There are many active internetworking research efforts both inside and outside of the Department of Defense (DoD). The Marine Corps' Tactical Data Network (TDN) must fit within the overall joint tactical internetworking architecture [JIEO,95a] and must be integrated into the global Defense Information Infrastructure (DII) [DISA,95] which encompasses all information systems throughout DoD. Therefore, the internetworking initiatives of the other military services, the Defense Information Systems Agency (DISA), and the global Internet community, as well as general trends in internetworking technology must all be considered by the Marine Corps in formulating its migration strategy for TDN. This chapter provides an overview of the development of the Internet Protocol and its role in current DoD networks. Also included are brief summaries of several recent and ongoing studies that complement and overlap this thesis.

B. BACKGROUND

1. History of the Internet Protocol (IP)

In the 1970s the Defense Advanced Research Projects Agency (DARPA) initiated an effort to develop a protocol that would permit the interconnection of disparate computer networks, each of which used a different underlying network technology. The central protocol produced by this project was the Internet Protocol (IP). The same research project developed several other higher level protocols designed to work hand-in-glove with IP. The most important of these was the Transmission Control Protocol (TCP), and the entire group of protocols was dubbed the TCP/IP protocol suite. [Cerf, 90]

The TCP/IP protocols were originally implemented the ARPANET packet switched research data network. The popularity of TCP/IP ballooned after the University of

California at Berkeley began incorporating TCP/IP into its version of the UNIX operating system. Since Berkeley UNIX was used in many universities' computer systems, TCP/IP became widely adopted. In 1986 the National Science Foundation network (NFSNET) was created, tying many more research facilities together using TCP/IP. As the NFSNET-ARPANET grew into the global Internet, TCP/IP gained unstoppable momentum. [Comer,95]

2. Department of Defense Adoption of IP

Declining defense budgets, the rapid pace of computer technology advances, and increased need for interoperability all led the Department of Defense (DoD) to adopt a policy of seeking commercial off-the-shelf (COTS) solutions to its computer systems needs. To control software costs, there was a push to build applications on common operating systems instead of developing each application from scratch. UNIX was the operating system chosen for most tactical command, control, communications, computer, and intelligence (C4I) systems.

TCP/IP's proliferation on the global Internet and the Defense Data Network (DDN), as well as its affiliation with UNIX, made it the logical choice for a standard DoD internetworking protocol suite. The sticking point was that the U.S. Government had mandated that all government information systems use the Government Open System Interconnection Profile (GOSIP), a collection of protocols that did not include TCP/IP [JIEO,95a]. Most of the protocols in GOSIP were defined by the International Organization for Standards (ISO). Although they were defined in the 1970s and early 1980s, and unlike IP, ISO protocols had never become widely implemented. In 1993 GOSIP was modified to include TCP/IP as alternatives to the equivalent ISO protocols [JIEO,95a].

It is clear that TCP/IP is DoD's protocol suite of choice for the near term. In 1995 the Defense Information Systems Network (DISN), the world-wide DoD data communications backbone, transitioned completely from X.25 (an ISO protocol) packet

switches to IP routers and gateways. Further, each of the four military services are developing and fielding tactical data switching systems based on the TCP/IP protocols [MCCDC,95b].

C. TERMINOLOGY

Several internetworking terms are used so frequently throughout this thesis that they are explained here for clarity. Additional aconyms and definitions appear in Appendix B.

host or ***end-system***	a consumer of network communications services. A host typically executes applications and server software programs on behalf of users and employs network communications services in this function. Hosts are usually individual workstations or personal computers (PCs). [MCCDC,95b]
internet	a collection of packet-switching networks interconnected by routers. [Comer,95]
Internet	The collection of networks that spans the globe and uses TCP/IP protocols to form a single, cooperative virtual network. When written in upper case, "Internet" refers specifically to this global Internet. [Comer,95]
internetworking	interconnecting many disparate physical networks and making them function as a coordinated unit [Comer,95].
node	a term applied to both routers and hosts [Perkins,96b].
protocol	a standard procedure or set of rules for defining and regulating data transmission among computers (or among different protocols) [Bradner,96a].

router a special-purpose dedicated computer that interconnects two or more networks and forwards IP datagrams from one to the other [Comer,95] Routers are distinct from hosts because they are usually not the destination of data traffic. Routing of IP datagrams is actually done in software. Therefore, the routing function can be performed by a host that has two or more network connections (dual-homed or multi-homed host). [MCCDC,95b]

World-Wide Web a world-wide virtual information space accessible via the Internet. Currently, the ***WWW*** or ***Web*** is composed of hypermedia documents (files) distributed on servers throughout the Internet. Users retrieve and view these hypermedia documents using client-server applications known as ***Web browsers***. [Hughes,94]

D. RELATED WORK

This section contains brief summaries of recent and/or ongoing research in the internetworking field that is relevant to the Tactical Data Network.

1. Tactical Internet Protocol Addressing Studies

Two recent studies completed within DoD have direct bearing on the TDN.

- ***Integrated Tactical-Strategic Data Network (ITSDN) Internet Protocol (IP) Addressing Plan*** [JIEO,95b] - Study undertaken by DISA's Joint Interoperability Engineering Organization (JIEO). The ITSDN plan assigns IP addresses for the routers at DISA communications facilities around the world where the tactical internets of deployed forces can be connected to the DISN and (by extension) to the Internet.

- ***IPAddressing Study*** [NCCOSC,95] - Study commissioned by Navy Space and Naval Warfare Systems (SPAWAR) directorate and carried out by the Naval Command, Control and Ocean Surveillance Center (NCCOSC) to determine how IP addresses should be allocated among Navy ships and shore communications

facilities. Completed in December 1995, the results of study are documented in a series of papers under the main title "IPADD." The main paper within the series assigns specific IP addresses to each ship and shore station. Other supporting papers discuss the implications and considerations of routing, security and bandwidth limitations on the Navy's IP network.

2. Internet Protocol version 6 (IPv6) Research

The development of IPv6 affects many other protocols. Although IPv6 research is not confined to the group cited here, this group maintains connections with all other IPv6 research efforts and is therefore a clearinghouse for current work in this area.

- ***Internet Protocol Next Generation (IPng) Working Group*** [IETF,96] - working group of the Internet Engineering Task Force (IETF), a voluntary organization of technical professionals who develop and refine protocols used in the Internet. The IPng Working Group is active in developing the detailed specifications for the next generation Internet Protocol, now formally called IP version 6 (the current version of IP is IPv4). The working group maintains two home pages on the World Wide Web. One is a subsidiary of the IETF's Web page and contains the group's official charter and a report of current status of IPv6 protocol specifications documents. This page is available at *http://www.ietf.cnri.reston.va.us/html.charters/ipngwg-charter.html* [IETF,96]. The other IPng Working Group Web page contains more general information about IPv6, an on-line overview, and a report on the current status of IPv6 software implementations. This page is available at *http://playground.sun.com/pub/ipng/html/ipng-main.html* [Hinden,96].

3. Related Internetworking Studies

This sections lists a number of internetworking studies completed by military officer students at the Naval Postgraduate School (NPS) who are members of the NPS Information Infrastructure Research Group (IIRG) [IIRG,96].

- ***Interoperability of Palmtop Computers with the U.S. Marine Corps Data Automated Communications Terminal (DACT) to Rapidly Disseminate Combat Order Message Packets Over Wired and Wireless Channels*** [Cummiskey,96] - Masters thesis proposing new software applications that can effectively disseminate operations orders using wireless links across the Marine Corps' tactical internet.

- ***Internetworking: Economic Storage and Retrieval of Digital Audio and Video for Distance Learning*** [Tiddy,96] - Masters thesis comparing the various existing multimedia compression methods and their potential use in creating multicast on-demand multimedia across an internet.

- ***Internetworking: Planning and Implementing a Wide-Area Network for K-12 Schools*** [Bigelow,95] - Masters thesis detailing how to get connected to the Internet, including comparison and analysis of the many LAN/WAN design choices that must be made in internetworking.

- ***Internetworking: Recommendations on Network Management for K-12 Schools*** [Trepanier,95] - Masters thesis detailing the many aspects of managing networks that are connected to the Internet.

III. TACTICAL DATA NETWORK (TDN)

A. INTRODUCTION

The Tactical Data Network (TDN) is a data routing system designed to interconnect end-user computers via local-area networks (LANs) and interconnect LANs to form a tactical internet. TDN equipment will extend this internet to every Fleet Marine Force unit, battalion level and above. This chapter describes the Tactical Data Network and how it fits into the overall Marine Corps tactical C4I architecture.

B. FLEET MARINE FORCE STRUCTURE

Since the 1930s the fighting forces of the Marine Corps have collectively been called the Fleet Marine Force (FMF). This emphasizes the fact that operational control of Marine forces is exercised primarily by Navy fleet commanders. Marines fight in composite units called Marine Air-Ground Task Forces (MAGTF, pronounced "mag-taff"). Each MAGTF is comprised of a Command Element (CE), a Ground Combat Element (GCE), an Air Combat Element (ACE), and a Combat Service Support Element (CSSE). The size of the MAGTF dictates the size of each of the elements. Currently, there are two basic MAGTF organizations used throughout the Marine Corps: the Marine Expeditionary Force (MEF) and the Marine Expeditionary Unit (MEU). The doctrinal organizational structures of the MEF and the MEU are shown in Figure 3.1.

There are three standing MEFs located throughout the world: I MEF in Camp Pendleton California, II MEF in Camp Lejeune North Carolina, and III MEF in Okinawa Japan. There are also standing MEU command elements within each MEF. Each MEU is subordinate to its parent MEF and is comprised of forces taken from among the MEFs units. MEUs normally deploy aboard Navy amphibious shipping to provide forward presence and an initial amphibious strike capability to Unified Combatant Commanders. The MEF is the basic warfighting unit of the Marine Corps and is the unit of interest in this study.

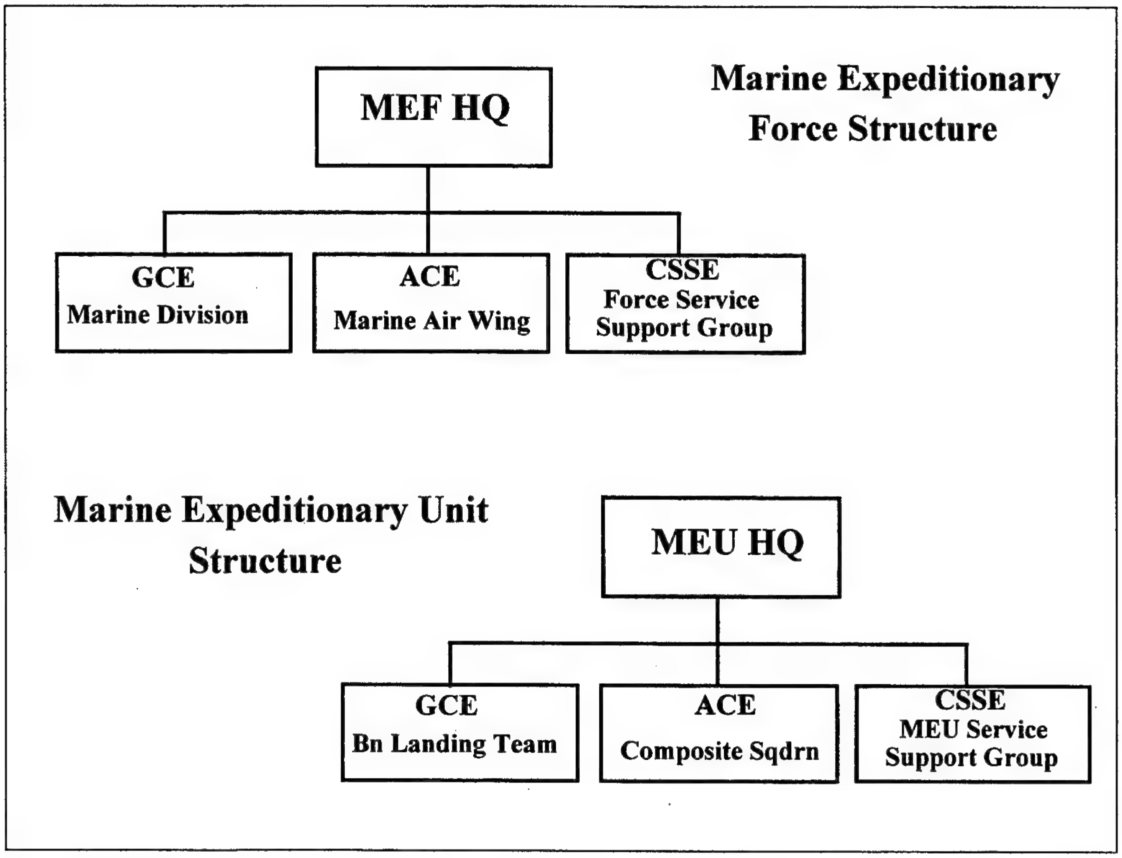

Figure 3.1 Marine Air-Ground Task Force (MAGTF) organizational structures.

C. MAGTF C4I

MAGTF C4I is the Marine Corps' strategy for achieving the midterm goal of the Joint Staff's *C4I for the Warrior* concept [Joint Staff,93]: a joint network of networks based on a common network operating environment using commercial standards. MAGTF C4I is the conceptual framework within which the Marine Corps is developing, acquiring, and employing command, control, communications, computers and intelligence systems. [MCCDC, 95b]

D. MAGTF C4I COMMUNICATION ARCHITECTURE

The Tactical Data Network (TDN) will fit within the existing and planned MAGTF communication architecture. The MAGTF architecture (Figure 3.2) is composed of transmission systems, multiplexing equipment, switches, and subscriber equipment. At the top of the layered architecture are the end systems which interact with tactical users and host the applications software. The end systems gain access to the data or voice networks via either switches or dedicated lines. TDN is the only data-switched network in the planned architecture. The multiplexing equipment and transmission systems are the physical communications means used to interconnect switches and end systems [MARCORSYSCOM, 95a].

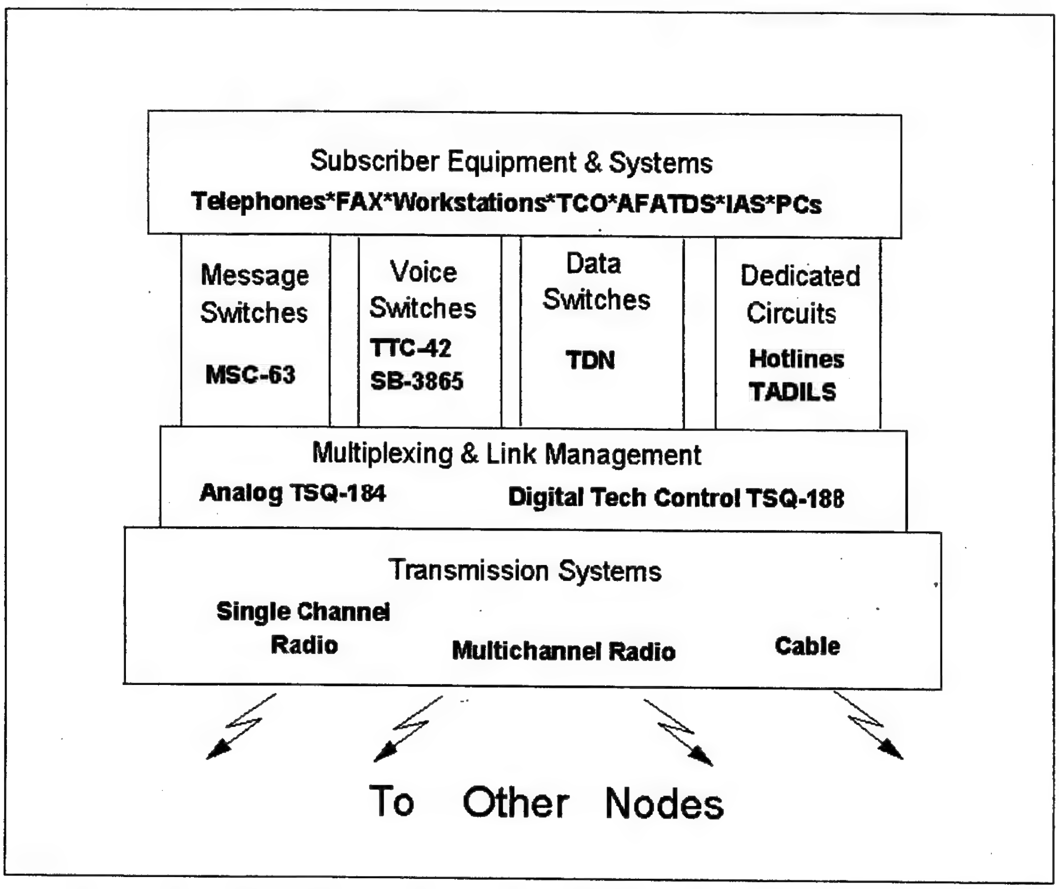

Figure 3.2 MAGTF C4I Communications Hierarchy. After [MARCORSYSCOM,95a]

1. External Network Connectivity

TDN is designed to provide seamless internet services within a tactical joint task force environment. It will interoperate with the other services' tactical packet-switching systems, as well as with strategic-level networks. Some of the specific networks that TDN will interoperate with are briefly described below.

a. Defense Information Systems Network (DISN)

DISN is an evolving world-wide data network that will ultimately provide the communications path for electronic mail, the bulk of DoD message traffic, and long-distance client-server applications such as browsing the World Wide Web. DISN is comprised of several networks, each operated at a different security classification:

- **Non-secure Internet Protocol (IP) Router Network (NIPRNET)** - NIPRNET is the unclassified packet-switched network operated by DoD. It has interconnections with the global Internet. Some tactical Marine Corps users will use TDN to access NIPRNET. [DISA,95b]
- **Secure IP Router Network (SIPRNET)** - SIPRNET is the SECRET packet-switched network of DoD. SIPRNET provides the communications backbone for the Global Command and Control System (GCCS), which will extend down to Marine Corps units via the TDN. [DISA,95b]
- **Joint Worldwide Intelligence Communications System (JWICS)** - JWICS replaced DSNET3 as the TOP SECRET SCI data network of the DISN. There is currently no requirement for TDN to provide SCI-level data services. The network connectivity for SCI traffic will be provided by dedicated systems such as Trojan SPIRIT. [DISA,95b]

▪ **Automatic Digital Network (AUTODIN) -** AUTODIN is DoD's secure record message system. It will be phased out in the coming years as the Defense Message System (DMS) is phased in. In the near term AUTODIN messages will enter the tactical area via special message-switching equipment (AN/MSC-63A). The DMS Multi-Function Interpreter (MFI) will translate AUTODIN messages into electronic mail which can be delivered via tactical packet-switched networks. Therefore, there is no need for TDN to interface with AUTODIN. [DISA,95b]

b. Integrated Tactical-Strategic Data Networking (ITSDN)

ITSDN is not a specific data-switching system. It is an umbrella term for the interconnection of all tactical packet-switched networks and their interconnection with with DISN. ITSDN will consist of IP routers at specific DoD communications facilities around the globe which will provide DISN entry points to deployed tactical commands. TDN is considered part of ITSDN and must be able to interface with the entry-point equipment. [JIEO,95b]

c. Tactical Secure Data Communications (TASDAC)

TASDAC is the data-switching system employed by the Joint Communication Support Element (JCSE) in Joint Task Force Headquarters. This system is also currently used by the Air Force for tactical data switching. TASDAC currently employs Wellfleet routers and is based on TCP/IP protocols. TDN must interoperate with TASDAC. [MARCORSYSCOM,95a]

d. Communications Support Systems (CSS)

CSS is the Navy's data communications system which extends IP networking to ships. TDN must interoperate with CSS both afloat and ashore. [MARCORSYSCOM,95a]

e. Tactical Packet Network (TPN)

TPN is the Army's tactical packet-switched network. TPN is overlaid on the Mobile Subscriber Equipment (MSE) system and operates at the SECRET classification level. TDN must be prepared to interconnect with TPN. [JIEO,95a]

2. Tactical Data Systems and End Users

The end users (i.e. customers) of TDN are primarily the tactical data systems (TDSs) that are being developed and fielded concurrently with TDN. These systems and corresponding requirements on TDN are examined in the next chapter.

E. TACTICAL DATA NETWORK SYSTEM DESCRIPTION

1. TDN Functions

The mission of TDN is to provide the MAGTF Commander an integrated tactical internet forming the communications backbone for all MAGTF tactical data systems [MARCORSYSCOM,95a]. This network will facilitate the seamless exchange of information across all echelons of command. TDN will be capable of supporting file sharing, information exchange, electronic message handling, and transport protocol translations. TDN must handle transparent routing of messages among LANs, circuit-switched networks and radio networks. [MARCORSYSCOM,95c]

2. TDN Subsystems

Two subsystems comprise the Tactical Data Network: the *TDN Gateway* and the *TDN Server*. Each of these subsystems has a different purpose and a different equipment configuration. Together a network of TDN Servers and TDN Gateways fulfills the TDN functional and operational requirements.

a. TDN Gateway

The primary purpose of the TDN Gateway subsystem is to connect Marine Corps internal networks to the external networks described in Section C. The TDN Gateway

a. TDN Gateway

The primary purpose of the TDN Gateway subsystem is to connect Marine Corps internal networks to the external networks described in Section C. The TDN Gateway will also interconnect multiple TDN Servers at Division, Wing and FSSG command posts. Subscriber LANs can also be connected directly to the Gateway, but that configuration is not recommended by the concept of employment.

Each TDN Gateway consists of two complete but physically separate suites of network equipment in one shelter. This allows a single TDN Gateway to support both a SECRET and an UNCLASSIFIED network simultaneously. The actual security architecture has not yet been decided, but it is likely that one physical network will carry data traffic of different security classifications [JIEO,95a]. Separation of the data traffic by classification level is accomplished by encrypting at least one of the data streams before injecting it into the shared network. This technique is called tunneling and is commonly used in packet-switched networks to allow two or more virtual networks to share a common physical network. TDN will transport TOP SECRET traffic by tunneling it across either the SECRET or UNCLASSIFIED networks.

The TDN Gateway is a shelterized system mounted on its own High Mobility Multipurpose Wheeled Vehicle (HMMWV). The Gateway has its own environmental control unit (ECU) and a pair of uninterruptable power supplies (UPSs). The internal logical layout of the Gateway subsystem is depicted in Figure 3.3.

At the heart of the system are two Cisco 7000-series enterprise routers. There are five UNIX workstations in the TDN Gateway that are capable of acting as LAN servers, providing network management functions, and hosting Domain Name System (DNS) and Defense Message System (DMS) software. The four Tactical Communication Interface Modules (TCIM) in the TDN Gateway provide the capability to connect remote and mobile hosts via half-duplex radio nets. Dial-in access interfaces are included to allow connection of subscribers from the circuit-switched TRI-TAC network. Finally the

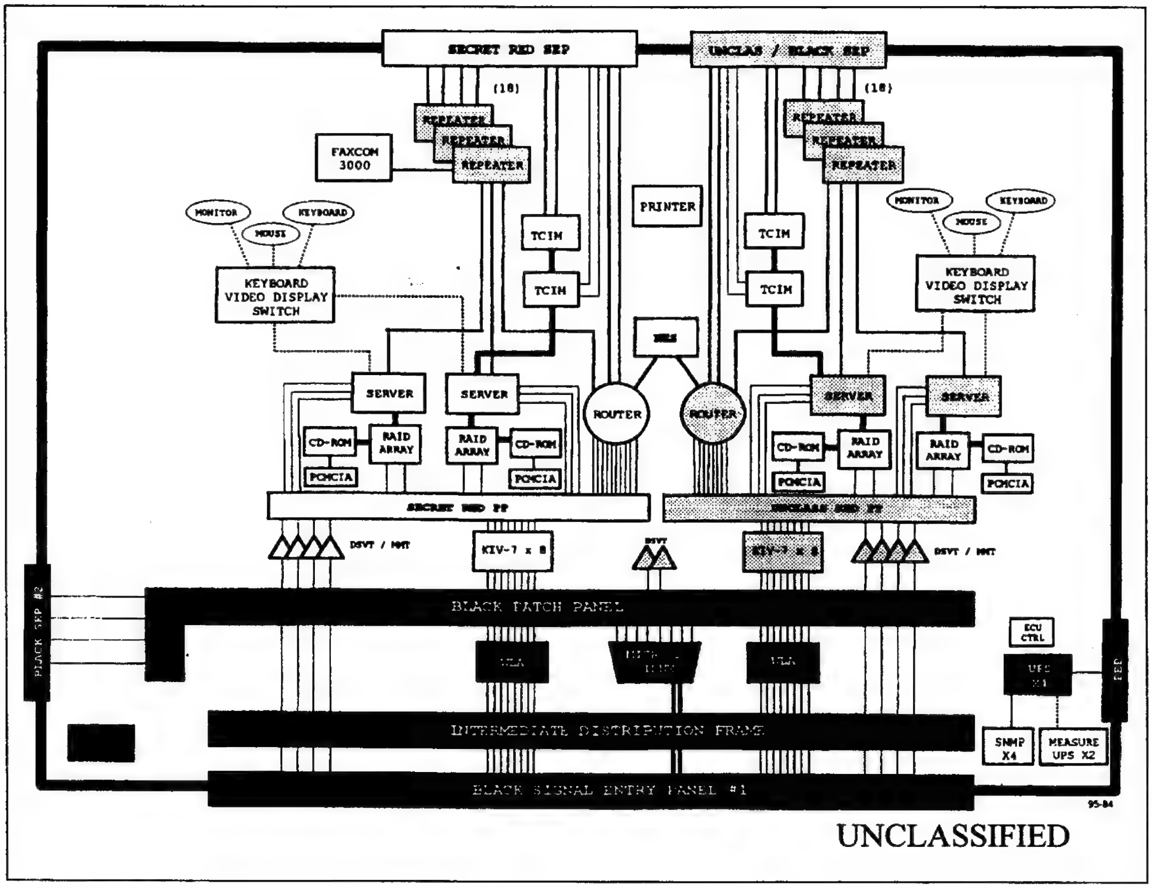

Figure 3.3 Tactical Data Network Gateway Block Diagram. From [MARCORSYSCOM,95c].

equipment suite is rounded out by KIV-7 encryption devices, serial wireline adapters, several LAN repeaters, a printer, and signal/patch panels. Although it is shown in Figure 3.3, the Motorola Network Encryption System (NES) is not a standard component part of the TDN Gateway.

b. TDN Server

"Server" is really a misnomer for this subsystem. The TDN Server provides functions similar to the TDN Gateway but on a smaller scale. The primary purpose of the TDN server is to connect individual subscribers to the tactical internet. Whereas the TDN Gateway can be thought of as a wide-area networking system, the TDN Server is a

local-area networking system. Each TDN Server provides the capability to establish a single LAN at a single security classification. Users operating at other security levels will have to connect to the TDN Server via an inline encryption device such as the Motorola NES.

The logical layout of the TDN Server is shown in Figure 3.4. The TDN Server is transported in three transit cases. One case contains a Cisco 2500-series router and UNIX workstation. The TDN Server provides radio access to the network via TCIMs, but does not provide any facility for dial-in access. The four removable LAN hubs allow each TDN Server to connect up to 48 network subscribers in four clusters of twelve. The hubs can be daisy-chained or connected directly to the router with Ethernet cable via the repeater. The TDN Server workstation functions as a LAN file server or groupware server, Domain Name System (DNS) server, and a Defense Messaging System (DMS) Message Transfer Agent (MTA). [MARCORSYSCOM,95a]

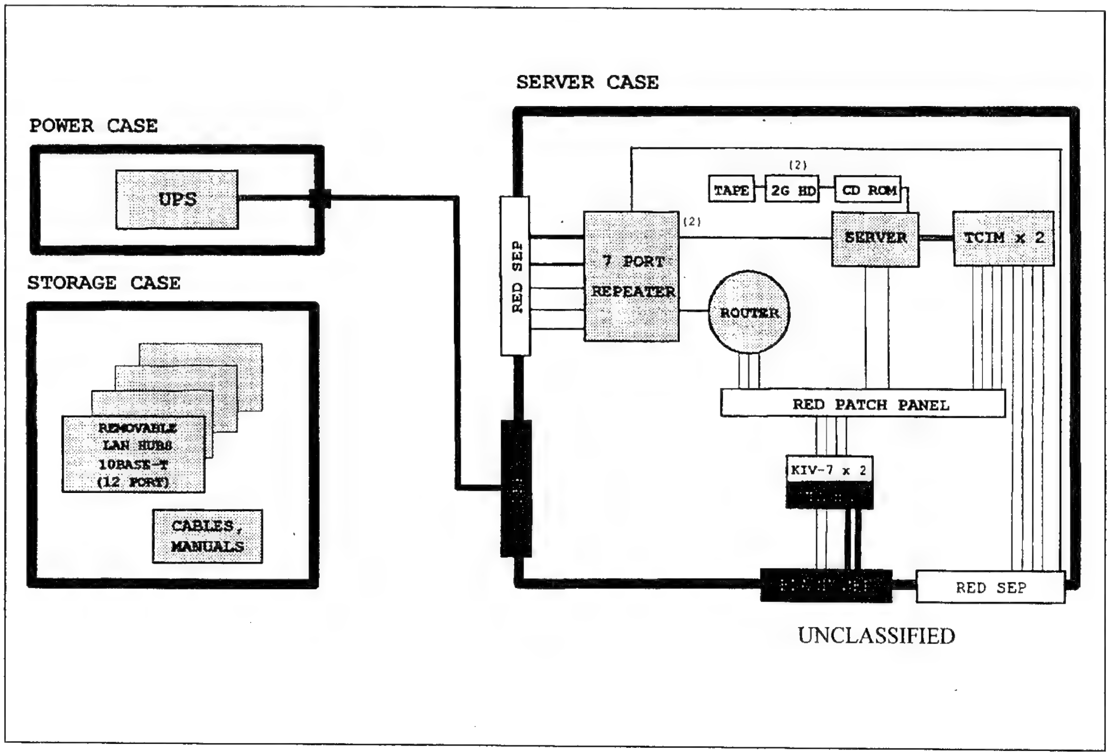

Figure 3.4 Tactical Data Network Server Block Diagram. From [MARCORSYSCOM,95a]

3. TDN Concept of Employment

The Tactical Data Network will provide a means to internetwork all of the tactical data systems within the Marine Air-Ground Task Force (MAGTF). It will also internetwork deployed Fleet Marine Force units with in-theater joint information systems, strategic level defense networks, and (optionally) the global Internet. Figure 3.5 depicts the logical interconnection of command posts using TDN. TDN will make it technically possible for a company commander using a hand-held computing device to exchange data with the National Military Command Center (NMCC). Operationally, TDN is expected to fulfill more limited needs.

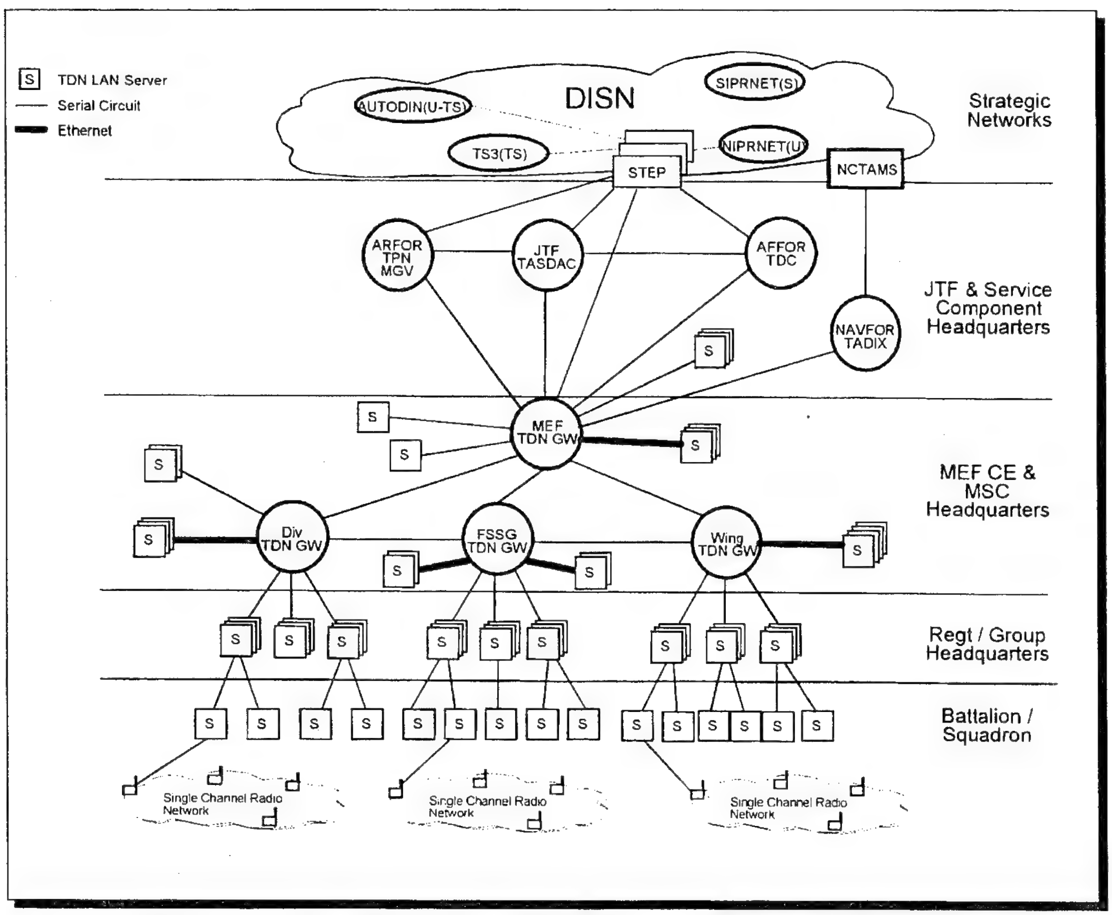

Figure 3.5. Tactical Data Network (TDN) interconnectivity to joint networks. From [MARCORSYSCOM,95a]

TDN Gateway subsystems will be deployed only at Marine Expeditionary Force (MEF), Marine Division, Marine Air Wing (MAW), and Force Service Support Group (FSSG) headquarters. TDN Server subsystems will be fielded to all units battalion-level and higher.

F. SUMMARY

The Tactical Data Network will bring about a quantum leap forward in Marine Corps tactical communication. Serving as the primary data switching system within the MAGTF, TDN will interconnect all end-user tactical data systems and all local-area networks into a seamless tactical internet. Although the general type of equipment that will be used in TDN has been decided, TDN's concept of employment and precisely how it will interface with all of its constituent end systems is not yet clear. The next chapter discusses future requirements that tactical end users and end systems will place on the Tactical Data Network.

IV. INTERNETWORKING MARINE TACTICAL DATA SYSTEMS

A. INTRODUCTION

Communications is driven by user requirements, not by technology. Network designers must look at who the users of the Tactical Data Network (TDN) are going to be before assessing the kind of technology that needs to be employed. The real users of TDN will be the commanders, staff officers and Marines of the Fleet Marine Force. Users will interface with TDN via applications software running on end-user computer systems, which may be UNIX workstations, personal computers (PCs) or handheld terminals. These end-user software and hardware systems are the focus of this chapter.

Section B describes the major end user systems that are expected to use TDN for network connectivity. Most of these systems are still under development and will be fielded concurrently with TDN in the 1999-2000 timeframe. Internetworking requirements of the end-user systems are then discussed in Section C. In subsequent chapters these requirements are used as the basis for examining the suitability of the current and next-generation Internet Protocol (IP) for the TDN.

B. DESCRIPTIONS OF TACTICAL DATA SYSTEMS

1. Common Operating Environment (COE)

The increasing complexity of modern C4I systems makes it imperative that users and applications software are shielded from the details of the underlying network structure [MCCDC,95b]. The Common Operating Environment (COE) provides a common operating system and core set of software utilities that can be used by every tactical data system application. Software application programs need only be designed to the COE application programming interface (API), not written from scratch as before. Thus applications can be inserted as modules on any computing platform running the COE [MARCORSYSCOM,94]. The COE also provides the user with a common

graphical user interface (GUI) for all applications. As an example, Microsoft Windows™ is a commercial implementation of this same concept (albeit for a limited hardware set). The COE is fundamentally a client-server architecture. Client application processes may access server processes on any workstation, as long as a communications path exists between them. TCP/IP suite networking protocols are built into the COE operating system.

All major tactical data systems now under development within the Marine Corps are being engineered to use the Global Command and Control System (GCCS) COE [MCCDC,95b]. The GCCS COE evolved from the Navy's Joint Operational Tactical System (JOTS). The software underlying JOTS, known as the Unified Build, also formed the foundation for the JOTS successor, the Joint Maritime Command Information System (JMCIS). The Joint Staff selected the JMCIS COE as the "best of breed" COE for the GCCS. In order to both reduce its software maintenance burden and facilitate full interoperability with Navy and Joint TDSs, the Marine Corps decided to re-engineer many of its tactical data systems to incorporate the GCCS COE [MARCORSYSCOM,94]. Figure 4.1 depicts the conceptual structure of the COE that is incorporated in Marine Corps tactical data systems. The COE is built upon a common hardware suite and a POSIX-compliant UNIX operating system. The common GUI is implemented using X-Windows/MOTIF interface tools. All of these lower-level software components are commercial off-the-shelf (COTS) products. At a higher level are the core services provided to all applications:

- Communications/message processor
- Track database manager/correlator
- Local database manager
- Charting and tactical plotting (mapping)
- Security shell

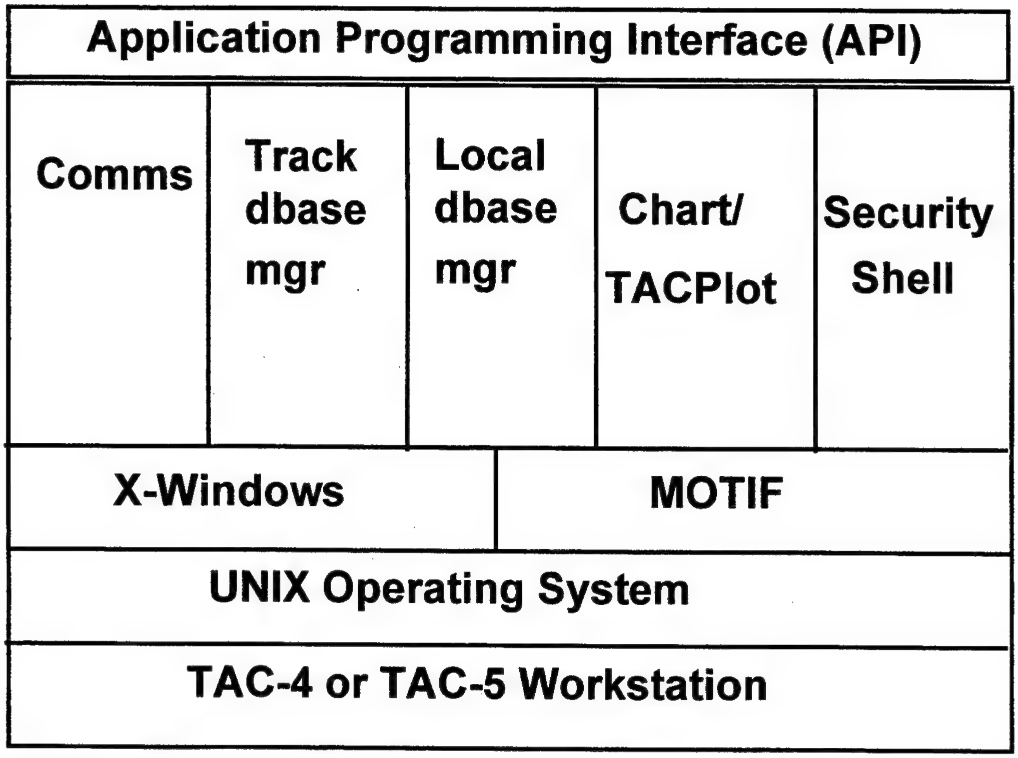

Figure 4.1 Global Command and Control System (GCCS) Common Operating Environment (COE). After [MARCORSYSCOM,94]

2. Global Command and Control System (GCCS)

GCCS is the system developed to fulfill the midterm goals of the *C4I for the Warrior* vision [DISA,96]. GCCS provides the warfighting Commanders-in-Chief (CINCs) and Joint Task Force Commanders (CJTFs) with automated support for planning, executing, and managing military operations. Fielded in 1995, GCCS replacing the Worldwide Military Command and Control System (WWMCCS) [DISA,96]. Within the Marine Corps, initial GCCS fielding was limited to garrison headquarters of the Marine Expeditionary Forces (MEFs) and Marine Expeditionary Unit (MEU) headquarters both ashore and afloat. In the future GCCS is envisioned to extend across all echelons of command [DISA,96].

3. Tactical Combat Operations (TCO)

TCO will be the primary tactical data system used by commanders and operations officers in the Fleet Marine Force (FMF). TCO will provide a fused real-time common operational picture (COP) of the battlespace. Establishing and maintaining this common operational picture will require much communication among the TCO systems within the MEF. Within a command center TCO will be hosted on workstations attached directly to local-area network (LAN) segments of the Tactical Data Network (TDN). When properly configured, a TCO terminal on the command post LAN can also serve as a wireless access point for mobile TCO users. Mobile TCO terminals may connect to the tactical internet via other TCO wireless interfaces or the wireless interfaces of the TDN infrastructure. These interfaces may accommodate connections from Single Channel Ground and Airborne Radio System (SINCGARS), Position Location Reporting System (PLRS), cellular phone, or any combination of these. TCO's functionality is similar to that of GCCS, and the two may eventually become indistinguishable. [MARCORSYSCOM,95a]

Among all tactical data systems, TCO will place the greatest communications demands on the Tactical Data Network (TDN). This is a function of both sheer numbers (TCO will exist in almost every tactical command center) and the types of applications TCO will run. In addition to maintaining the common operational picture, TCO is envisioned to support distributed collaborative planning (DCP). Distributed collaborative planning allows multiple commanders and staff members who are in separate command posts to collaborate in real time on the development and editing of a single operations plan. DCP will probably be applied tactically for concurrent development of courses of action and operations orders, both of which are functions of the objective TCO system. IP-compatible desktop videoteleconferencing (VTC) capability may also become an integral part of DCP [Macedonia,94]. The particular demands that technologies such as these place on the TDN will be discussed later in this chapter.

4. Intelligence Analysis System (IAS)

IAS provides automated support for the direction, collection, processing, production, and dissemination of intelligence within the MAGTF. The system is scaleable from a single workstation at battalions and squadrons up to a suite of nine workstations at the MEF command center [MARCORSYSCOM,95a]. A portion of IAS will operate at the SECRET level and will therefore be incorporated into the TDN LAN/WAN. IAS has numerous capabilities, many of which employ the tactical internet. One of the uses of IAS is for accessing INTELINK-S. INTELINK-S is an intelligence information space that uses the same Hypertext Markup Language (HTML) format popularized by the World Wide Web (Web). Users access the INTELINK-S via the tactical internet utilizing a Web browser program. It is expected that intelligence personnel at the tactical level will use such methods to gather (i.e. "pull") information from the global infosphere.

5. Advanced Field Artillery Tactical Data System (AFATDS)

AFATDS is a computerized command and control (C^2) system for artillery units and Fire Support Coordination Centers (FSCC). It is being developed jointly by the Marine Corps and the Army. AFATDS will enable tactical and technical fire direction for artillery fires, as well as automated support for controlling air strikes and naval surface fire support. AFATDS will be hosted primarily on UNIX workstations in Fire Direction Centers (FDC) and Fire Support Coordination Centers (FSCC), but it will also be fielded to the Direct Air Support Center (DASC) and the Tactical Air Command Center (TACC). There will also be man-portable AFATDS terminals. The AFATDS terminals within a single command center form a distributed cooperative system that uses a local-area network (LAN) to communicate and exchange information. A single command center may have as many as eight AFATDS terminals. Although there is currently no definite fielding plan, it is anticipated that there will be 160-200 AFATDS terminals in each MEF. [Chmielewski,96]

Besides TCO, AFATDS will probably generate the greatest volume of data traffic within a Marine Division's tactical internet. The time-sensitive nature of fire support communications places unique demands upon a shared, connectionless communications system like TDN. This issue will be discussed in greater detail later in this chapter.

6. Advanced Tactical Air Command Center (ATACC)

ATACC is the primary C^2 system for the MAGTF's Air Combat Element (ACE) battle staff. It will support overall air warfare planning and execution for a MAGTF operation, and will interface with the Joint Task Force's air planning systems. The Contingency Theater Air Planning System (CTAPS) will be integrated into ATACC as the ACE's primary automated mission planning and analysis tool. CTAPS will assist the ACE staff in generating, disseminating, and manipulating the Air Tasking Order (ATO). The ATACC system itself consists of up to 30 UNIX workstations, 20 of which will be used for CTAPS. Remote CTAPS workstations will be operated at all squadrons and other major commands within the MEF. [MCTSSA,96]

7. Improved Direct Air Support Central (IDASC)

IDASC provides automated support for handling tactical air requests from Forward Air Controllers (FACs) and Air Liaison Officers (ALOs) within the Marine Division, as well as automated tools for parsing the Air Tasking Order (ATO). IDASC is hosted on UNIX workstations and will exist primarily at the Direct Air Support Center (DASC) in each MEF. [MARCORSYSCOM,95a]

8. Marine Combat Service Support Command and Control ($MCSSC^2$)

The Marine Combat Service Support Command and Control system is a logistics and personnel support system. It allows commanders of Combat Service Support (CSS) units to exercise command and control over their forces. $MCSSC^2$ will also be fielded to units within the Marine Division and Marine Air Wing to assist unit logistics officers in requesting and tracking CSS. [MARCORSYSCOM,95a]

9. MAGTF Tactical Warfare Simulation (MTWS)

MTWS is a transportable computer-assisted wargame designed to enhance training of Fleet Marine Force (FMF) commanders and their staffs. MTWS is hosted on a distributed network of UNIX workstations, typically linked by an Ethernet LAN segment. At least five workstations must be used to run MTWS. There can be as many as 30 workstations connected depending on the number of displays needed and the need to distribute the processing load of the simulation. In a deployed environment, where MTWS might be used to assist in course-of-action development, it is unlikely there will be more than five MTWS workstations deployed with each staff. [Sawyers, 95]

10.Other Systems

In addition to the major tactical data systems mentioned above, there will be many other users of the tactical internet. Although it is not possible to predict all of the systems that will connect to TDN, some systems that are likely to be supported are *PC Client*, Lotus Notes™ and Windows NT Server™.

PC Client is a software package developed by the Marine Corps Tactical Systems Support Activity (MCTSSA) that allows a personal computer (PC) to exchange common operational picture data with a TDS UNIX workstation. The purpose of *PC Client* is to reduce the number of relatively expensive UNIX workstations needed by the Fleet Marine Force. Whether or not the specific *PC Client* software is used in the future, the trend toward using internetworked personal computers will be fueled by the continuing advances of the PC industry in multitasking, processing power, memory capacity, and connectivity capability.

Currently, the Marine Corps uses Banyan Virtual Networking System (VINES)™ to network its personal computers in both garrison and tactical situations. In this system personal computers are internetworked using the proprietary VINES-IP protocol. Each PC has a VINES-IP address, but does not necessarily have a standard Internet Protocol (IP) address unless the user has a need for direct NIPRNET or SIPRNET access. The

Marine Corps near-term plan is to migrate to a PC networking system of Lotus Notes™ groupware running on the Microsoft Windows NT™ operating system. Notes™ allows several users (who may be separated by an internet) to simultaneously access and work on shared documents. Windows NT™ uses standard IP for internetworking. Therefore all personal computers in the MAGTF that access the tactical internet will require IP addresses. [Gaunter,96]

C. INTERNETWORKING REQUIREMENTS

This section examines some of the salient communications requirements placed on the tactical internet infrastructure by the end systems which were described in the previous section. It is difficult to know exactly what these requirements will be for two reasons:

- Most of these systems are still under development.
- Users often employ a fielded system differently than was anticipated by the system's designers.

Using what is known about these systems, in conjunction with the requirements stated in the TDN Operational Requirements Document (ORD) [MCCDC,95a], five broad areas of internetworking requirements were selected for analysis: *addressing, multicast communication, mobility, quality of service (QoS),* and *security.*

Much has already been written in the public domain about protocol requirements for the global Internet. Many of those requirements parallel those of the Marine Corps' tactical internet. There remain some areas (such as scalability) where the two requirements sets are not necessarily in consonance.

1. Addressing Requirements

Section B discussed only the major tactical data systems that will be deployed in the MEF. There will surely be many more workstations and PCs in the tactical environment as the Corps becomes a more information-intensive force. In order to have

a fully seamless and robust information grid, all of these systems will have to be interconnected and internetworked. Every end system must be capable of communicating with every other system in the internet. This requires that the network provide a unique means of identifying each end system. In an IP internet, this unique identifier is the IP address. Assigning IP addresses is a major task. Not only must the number of end systems be considered, but also the arrangement and employment of those systems. For example, systems such as AFATDS may require that all workstations at the same command center share the same local-area network (LAN) segment. Likewise, command elements are often organized into multiple command groups which operate separately (Forward and Main Command Posts). This kind of physical and logical separation must be accounted for when assigning IP addresses.

Assigning, reconfiguring, and tracking IP addresses can be a significant burden on network managers. This can be a serious problem in smaller units which may lack the manpower and expertise to do the job correctly. For this reason there is a requirement to keep IP address assignment and configuration as simple as possible. Ideally either configuration might be done automatically by the networking software, or address assignment would not change regardless of circumstance.

2. Multicast Requirements

The TDN ORD states that TDN must support multicasting [MCCDC,95a]. Multicasting is the transmission of a single copy of the same information to a *selected group* of stations on a network at the same time. Multicasting is really the general case of all communications. *Broadcasting* is a special case of multicasting in which the multicast group includes *all* stations on the network. *Unicast* communications involves transmission to only one station.

Multicasting is already used extensively in military communications. A SINCGARS radio net is an example of a multicast topology. Although the radio transmission is physically broadcast by the sender, only a select group of radios are

configured to receive the transmission. In an internet the difference is that not all of the stations who need to receive the information are connected by the same physical communications medium. The key advantages of multicast over unicast or broadcast are that it conserves bandwidth and requires less computer processing. Bandwidth is conserved because no data packet traverses a communications link more than once. Further, multicast data transmission does not even cross a communication link unless there is a station on the other side of the link that is a subscriber to the multicast group. By contrast, unicast requires a separate transmission for each receiving station while broadcasting sends packets everywhere regardless of actual receiving station locations. Conserving bandwidth is especially crucial in the tactical internet, where radio is often the primary means of communication and link capacities can be less than 9.6 kbps.

Multicast also consumes less computational resources at the receiving stations than broadcast. A packet with a *broadcast* destination address must be examined by every end-system computer that receives it. Most computer network interface hardware can be configured to only accept data packets destined for particular *multicast* addresses. By stopping unwanted data packets at the network interface card, the end system CPU is not burdened by examining and rejecting those data packets. In a shared data network like TDN this can be a significant advantage.

There are many examples of tactical data exchange that must be multicast. One is position update information that maintains the common operational picture for TCO, GCCS and other terminals. Another example is electronic mail that must be delivered to multiple recipients who all reside on the same destination network. Yet a third example is a distributed collaborative planning (DCP) session involving participants at several command posts, all of whom must be able to see the same data at the same time. DCP traffic can involve simultaneous audio, video, and data multicasts.

Global Broadcast Service (GBS) is another emerging technology that may require multicast. GBS is a high-power high-bandwidth system that permits ground stations to use small antennas to passively receive television and data. The unique aspect of data

transfer on GBS is that the receiving station does not have a full-duplex communication path with the data source via the GBS satellite. The receiving station must either establish a return path via other means (such as a modem and serial-line connection), or just receive the broadcast data one way. The networking protocols used must accommodate this asymmetric topology. [Morales,96]

A major issue in defining a multicast requirement is whether or not the communication must be *reliable*. Reliable in this sense means that the sender has a way of knowing that all intended destinations received the transmitted data, and receivers can account for all intended traffic. Position reporting may not need guaranteed reliability if the positions are changing slowly and the updates are being sent frequently. Audio and video streams rarely require reliability since a few missed "sound bytes" or picture frames do not significantly disrupt the overall impact of the communication. On the other hand, the sender of an e-mail message containing an intelligence image, operations order, or overlay must be assured that all intended recipients got it without error. Therefore, there are requirements in the tactical internet for both unreliable **and** reliable multicast.

Multicast does not just happen automatically. The internetwork infrastructure must support multicast, and the end-system applications must be configured to take advantage of the network's multicast capability. As the force moves toward a distributed, decentralized structure, the need for rapid, simultaneous information sharing will increase. The Marine Corps has stated that in future warfare "information will be originated once and shared by all" [WarLab,96]. Therefore many-to-many (multicast) communications will continue to increase in usage and importance relative to one-to-one (unicast) communications in the tactical internet.

3. Mobility Requirements

Greater mobility of land forces is expected to be a tenet of 21st century warfare. The Army has expressed this in its *Force XXI* concept [U.S. Army,96]. Likewise the Marine Corps stresses mobility in its current doctrine of *Operational Maneuver from the*

Sea and in a new concept for expeditionary warfare called *Sea Dragon* [WarLab,96]. This is stated clearly in the Sea Dragon concept paper:

> A significant increase in force mobility is required. Forces will have to be highly mobile in conducting the mission, and able to be rapidly extracted or relocated as the mission is completed. [WarLab,96]

The Tactical Data Network (TDN) will have to support several kinds of end system mobility. Individual computers will be moved around within each command center changing their physical network connections. Users must be able to relocate or replace their workstations in order to adapt to physical constraints, adaptive C^2 structures, and equipment failures. Entire units and their networks will also be mobile. A unit may simply physically relocate but remain part of the larger network, as in the case of a command post displacement. If displacement involves temporary loss of a networking node (router), the rest of the internet must dynamically adapt. The same unit may, however, move and become part of an entirely new network. A MAGTF headquarters moving from ship to shore is an example of this latter type of mobility. While afloat the MAGTF connects to the Joint Task Force (JTF) via the Navy's network. Once ashore the MAGTF sets up its own satellite or microwave internetwork connectivity to the JTF. While shifting locations, partial connectivity via wireless links may be needed. Unit mobility of this type can require substantial addressing and routing changes to the internet infrastructure.

Some individual end-user terminals will be nomadic, dynamically moving from network to network while maintaining continuous access to internet services. Users who are "roaming" will connect to the tactical internet via SINCGARS radio, wireless LAN, cellular phone, or a combination of these. Other mobile users will disconnect from the internet, move, and reestablish an internet connection in a new place.

Which users are mobile and which are not needs to be transparent to other network users. Keeping track of mobile users is a requirement for the network infrastructure

itself. Further, the mobile user should not have to take extraordinary measures to get connected and remain connected to the internet while roaming. The TDN ORD explicitly states a requirement to "provide the means for a mobile host to enter and leave the network with minimal user-performed system configuration changes" [MCCDC,95a]. Ideally, all adjustments will be dynamically and autonomously handled by the network, as they are in commercial cellular telephone networks.

4. Quality of Service Requirements

Some types of applications and end-user systems must have access to a certain amount of a network's resources in order to function properly. That is, they require a certain quality of service (QoS) from the network. By negotiating a quality of service guarantee, an end-user system can gain some control over an otherwise-shared network infrastructure.

Dimensions of network quality of service are usually discussed in terms of bandwidth guarantees, controls on the amount and variability of network-induced delay, and reliability provisions for ensuring error-free and in-order data delivery [Jeffries, 96]. All applications do not require the same QoS. Several emerging classes of applications that are being embraced by the military will require some QoS guarantees if they are to work in the tactical internet.

Recently, multimedia applications that involve transmission of audio and video across the network in real time have become popular in both the commercial and military sectors. The trend toward multimedia will continue and the tactical internet must therefore support multimedia and real-time applications. Multimedia applications place a high demand on the network infrastructure because they are intolerant of out-of-order data or long and/or inconsistent delay. In order to support such an application, a network must provide special handling of the data packets transmitted between the two ends of the connection, guaranteeing some minimum thresholds of bandwidth and latency to the application so that it can operate properly on a shared link.

Distributed collaborative planning (DCP) is an application area that is enjoying much interest and research. DCP can be facilitated by commercial groupware products such as Lotus Notes™ [Lotus,96] as well as by military-specific products such as the Theater-level Analysis, Replanning, and Graphical Execution Toolbox (TARGET), which will become part of GCCS [DISA,96]. Today's concepts of DCP range from two users remotely sharing a document on an electronic "whiteboard" to full-blown multipoint desktop videoteleconferences. Similar applications have been used to conduct seminars and meetings across the global Internet utilizing a virtual network known as the Multicast Backbone(MBone) [Jacobson,94]. (MBone will be discussed in the next chapter.) Intense interest in this technology suggests that it will continue to flourish in the future and will find applications in tactical C4I. For example, the command and coordination concept for *Sea Dragon* refers several times to the need to enable "dynamic collaboration among all elements" [WarLab,96]..

Distributed interactive simulation (DIS) is another application that may also require quality of service guarantees. It is not yet clear how prevalent simulation will be in tactical units. If simulations prove to add value at the tactical level, however, they will certainly be internetworked. Simulation architectures used for exercises can be used identically for actual engagements. Data transmission for DIS must be real-time, many-to-many multicast and reasonably reliable. [Bradner,96a]

All quality of service does not have to be provided in the network infrastructure. Reliability is often considered an end-system function [Comer,95]. Real-time multimedia applications have been developed that can adapt to some degree of packet delivery delay as well as to out-of-order packet delivery. However, there is a limit to what these applications can do, and thus delay caused by the network must be bounded.

Beyond the technical requirements of bandwidth and delay there is the issue of priority. Priority determines which traffic gets network resources regardless of the traffic *type*. Priority is a *policy* that needs a technical enforcement mechanism in the network.

In recent years tactical communication has consisted predominately of voice traffic transmitted over user-controlled, single-purpose radio and wire links. All users on those links shared a common purpose and enforced their own priorities through net control stations. With the fielding of TDN, much of the information that used to flow over those dedicated links will shift onto a shared data internet. Users will lose some control over their communications path. Consider an example from the Sea Dragon concept paper:

> Target information emanating from a dispersed small team might be injected by a FOFAC into a personal handheld computer for immediate transmission into the network, whereupon all agencies simultaneously receive that information for processing. [WarLab,96]

There is an implicit assumption in this scenario that such traffic will not become delayed or discarded by some network device whose queue is full of administrative traffic. There must be some means in TDN to ensure that the command's priority policies can be enforced in the network infrastructure.

5. Security Requirements

In this age of Information Warfare (IW) network security has become a heightened concern. There is consensus that information dominance holds the key to victory in next generation warfare. However, there is a dichotomy in our ambitions. On one hand, we want more information sharing as well as easier and faster access to information. At the same time we want greater security protection for that same information. Simultaneously fulfilling these two goals is a significant challenge.

Users have four general network security requirements: *confidentiality, authenticity, integrity,* and *availability* [Russell,91]. Users need their sensitive and classified data to remain *confidential*. Access to the data's content must be denied to unauthorized users. Users need assurance of data's *authenticity*, or proof of its time and place of origin. Data must retain its *integrity* and not become corrupted during

transmission or while in storage. Finally, data and network resources must be *available* to the user when he needs them.

Confidentiality is the facet of security that has always been stressed most strongly by the military. As attention has focused on IW, the military has better understood the relative importance of authenticity, integrity, and availability. The question in this study is whether there is a requirement for the network infrastructure itself to fulfill or support any of these security requirements. The vulnerability of the network's devices and controls is a key concern. Protection must be afforded to TDN routers and servers to ensure that the tactical internet remains available for use when critically needed.

There are a myriad of other specific security requirements in the tactical internet. There will be force-readiness databases, directories, and geoposition data that must all be protected. The data must retain its integrity, confidentiality and availability. User queries to these databases must be authenticated. Much of that security can be provided by the applications themselves. Lotus Notes™ , Windows NT™ and most of the tactical data systems have built-in security measures [Lotus, 96]. Multilevel security (MLS) features will be integral to the objective Defense Messaging System (DMS) [JIEO,95a]. Link encryption devices (KY gear) will continue to be employed at the physical communications level to scramble the data stream and prevent traffic analysis [JIEO,95a]. TDN must have an integrated security architecture that incorporates security technology where it is needed, but avoids proprietary methods and duplicative security overhead among layers.

D. SUMMARY

A great many end user systems will eventually connect up to the Tactical Data Network. Each will place different demands on the network infrastructure. These requirements are summarized in Figure 4.2. While the exact nature of future applications in the tactical environment cannot be known for certain, a clear pattern is developing. Technologies which appear in the commercial world and on the global Internet quickly develop advocates and applications within the military. Just one example of this is the

development of INTELINK, a classified information space identical in form to the enormously popular World Wide Web. There is no reason to doubt that this trend of technology transfer will continue in the future. *Sea Dragon's* focus on smaller, more mobile and fully networked forces, coupled with the shift toward information warfare also create unique network requirements. The tactical internet infrastructure of the next century must be capable of fulfilling all of these diverse requirements.

ADDRESSING	-Need IP addresses for the myriad of communicating devices in the tactical internet - Simple and dynamic method of assigning IP addresses
MULTICAST	- Common Operational Picture to everyone - Distributed Collaborative Planning (DCP) - Both reliable and unreliable multicast delivery - Conserve bandwidth on tactical links
MOBILE NETWORKING	- Accommodate "roaming" of mobile users - Handle intermittent communications links - Mobile routers as well as mobile terminals
QUALITY OF SERVICE	- Support real-time multimedia like DCP - Support prioritization by data type as well as data source - Guarantee bandwidth available for critical applications
NETWORK SECURITY	- Ensure confidentiality, integrity, authenticity of data - Protect network infrastructure from attack

Figure 4.2 Summary of the internetworking requirements of tactical data systems.

V. INTERNET PROTOCOL VERSION 4

A. INTRODUCTION

This chapter examines aspects of the current Internet Protocol (IPv4) that are relevant to the Tactical Data Network (TDN) requirements discussed in Chapter III. The objective of this chapter is to identify which requirements of TDN that can be met by IPv4 and which cannot. The analysis focuses on the concepts and capabilities of the Internet Protocol, rather than on the specific protocol details.

Complete details of IPv4 and the entire TCP/IP protocol suite are contained in original documents known as the *Request for Comments* (RFCs) series. All RFCs are available online at *ftp://ds.internic.net/rfc/*. The Department of Defense (DoD) has established *profiles* for several TCP/IP protocols that assign specific values to the protocols' options and/or parameters. These profiles are published as military standards (MIL-STDs) in the MIL-STD-2045-xxxxx series [MCCDC,95b]. All MIL-STDs are available online from the DISA Center for Standards at *http://www.itsi.disa.mil*.

B. OVERVIEW OF IP VERSION 4

1. The Need for an Internet Protocol

A protocol is a rule that two or more computer systems must agree upon and adhere to in order to exchange data unambiguously [Comer,95]. For example, in data communications there must be a protocol that defines how a computer system interfaces with the physical communication medium to which it attaches. Such data link (or network interface) protocols are often limited by the details of the particular networking hardware used. In an internet, however, end-user computing systems must communicate across heterogeneous intermediate networks that may incorporate widely disparate hardware technologies, such as Asynchronous Transfer Mode (ATM), single channel radio, Fiber Distributed Data Interface (FDDI) and Ethernet. In a truly open system

architecture, end-user host machines and user-level applications cannot be required to deal with the complexity and heterogeneity of the underlying internetwork. A protocol is needed that transcends the details of the various technologies and vendor implementations of physical networks, thus presenting the end user with a common abstraction of the network. This is the purpose of the Internet Protocol.

2. IP's Placement in the Protocol Stack

Communicating data across a network is too varied and complex a task to be accomplished through use of a single protocol. Protocol layering partitions the communications problem into bounded, manageable tasks. Although not widespread in implementation, the Open System Interconnect (OSI) 7-Layer Reference Model (Figure 5.1) developed by the International Organization for Standardization (ISO) is the most commonly referred-to abstraction for protocol layering.

Layer	Functionality
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical Connection

Figure 5.1 The Open System Interconnect (OSI) 7-Layer reference model. After [Comer,95].

The original purpose of this model was to guide ISO protocol development committees in bounding the scope of their protocols [Buddenberg, 95]. The protocol at each layer only needs to define the interface with the next higher and next lower protocol layers. This permits network hardware implementation details to be hidden from the applications software and end users.

However, the OSI model does not accurately describe the layering of the TCP/IP protocol suite. The TCP/IP protocols do not map neatly into seven layers because the Defense Advanced Research Project Agency (DARPA) developed TCP/IP independently of the OSI model. The TCP/IP protocol stack is conceptually divided into four layers: *Applications* or *Processes*, *Transport*, *Internet*, and *Network Interface or Data Link*. Figure 5.2 is a conceptual comparison of the TCP/IP and ISO models.

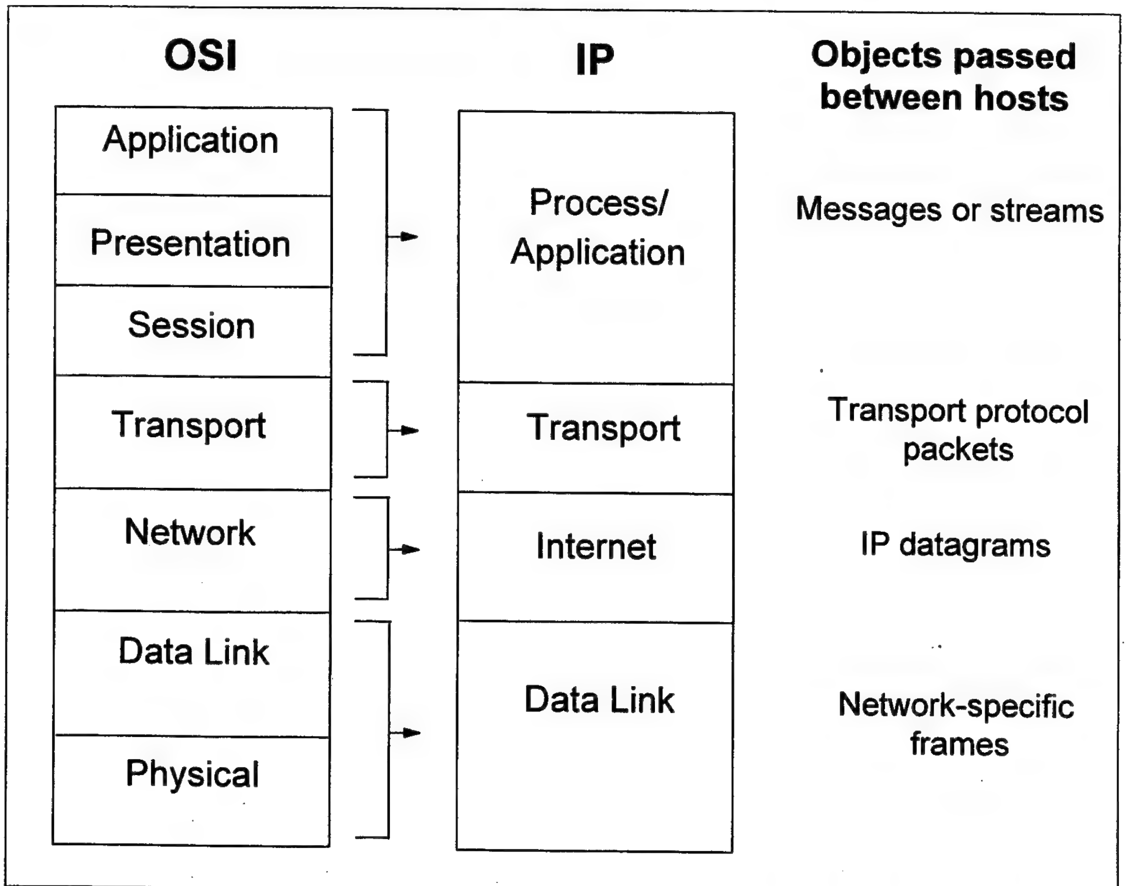

Figure 5.2 Correspondence between OSI and IP protocol layer models, and information objects passed between corresponding host layers. After [Brutzman,96]

Because the OSI model was intended to describe communications in a single network, it contains no specific *internet* layer (IP) [Comer,95]. Furthermore, the TCP/IP layers are not as strictly constrained as those in the OSI stack. OSI protocols can only communicate with protocols in adjacent layers. By contrast, any TCP/IP layer can interface directly with any other layer. Implementing this feature can greatly reduce overhead in certain situations and makes TCP/IP more flexible than OSI [Brutzman, 96].

IP's mapping into the ISO model is not as important as IP's relationship to the other protocols that will be employed in the tactical internet. Figure 5.3 shows the dependency of all projected tactical applications upon IP for network communications.

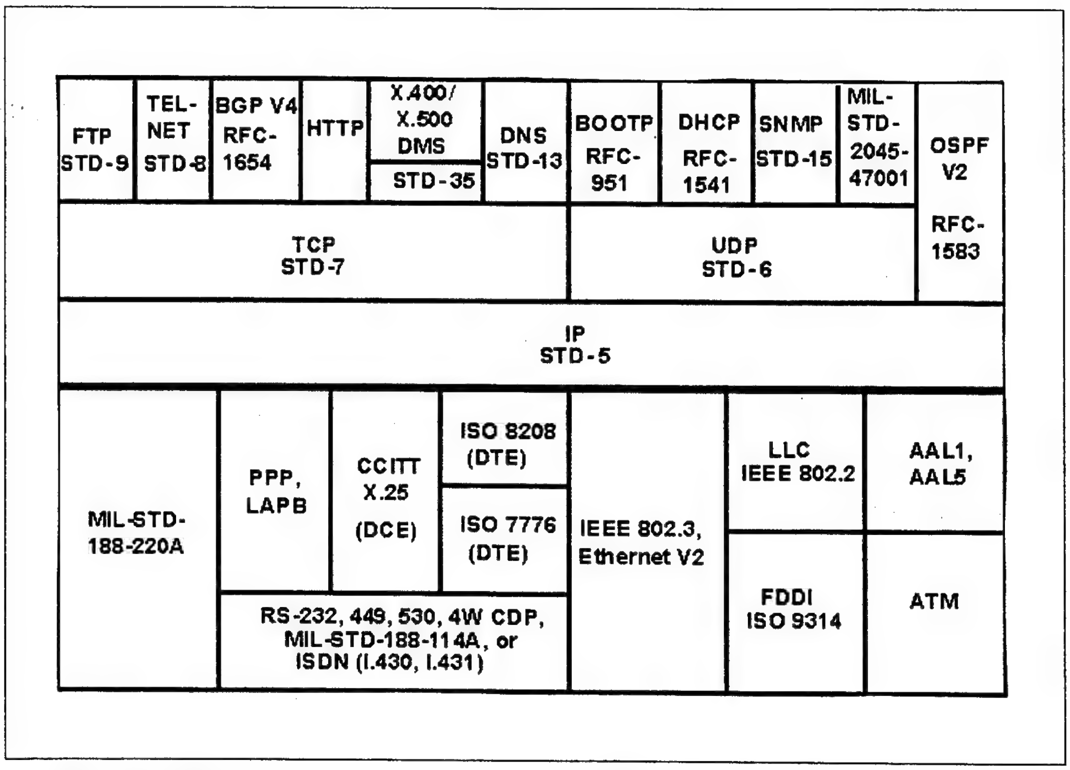

Figure 5.3 Protocol layering in the tactical internet. These layers map directly to the four-layer IP stack in Figure 5.2. From [Dept. of the Army,95]

The figure also illustrates the broad range of network hardware interface (data link layer) protocols with which IP can interoperate. Only a few of the protocols shown in Figure 5.3 will be discussed in this thesis. A list of acronyms is provided in Appendix B.

3. The Internet Protocol as a Bearer Service

A bearer service is a protocol abstraction of the underlying data communication network. The main characteristic of the bearer service is that it decouples the higher level applications from the lower level hardware technology. Described in "Realizing the Information Future: the Internet and Beyond" [NRC,94], the concept of the bearer service is illustrated in Figure 5.4. The importance of the bearer service is obvious from its place at the neck of the "hourglass" figure. This centrality is a powerful feature. It allows higher and lower technologies to evolve independently as long as they can all interconnect via the bearer service. However, since the bearer service must be agreed upon by everything above and below it, the bearer service must be sparse and simple. [NRC,94]

The authors of "Realizing the Information Future" admit that they used the Internet Protocol (IP) as their model for the bearer service [NRC,94]. IP is the bearer service for the global Internet, and was specifically defined independently of any particular technology. IP datagrams are typically processed in software, so their format and content are not constrained by the details of any hardware. This has enabled IP to accommodate the introduction of various new hardware and software technologies. The Internet Protocol per se is also quite simple. It really only defines two things: the datagram structure (hence IP address) and the connectionless packet delivery service.

4. IP's Connectionless Data Packet Delivery Service

The IP layer supports connectionless (as opposed to connection-oriented) data transfer. Conceptually, an IP internet operates like a more familiar connectionless

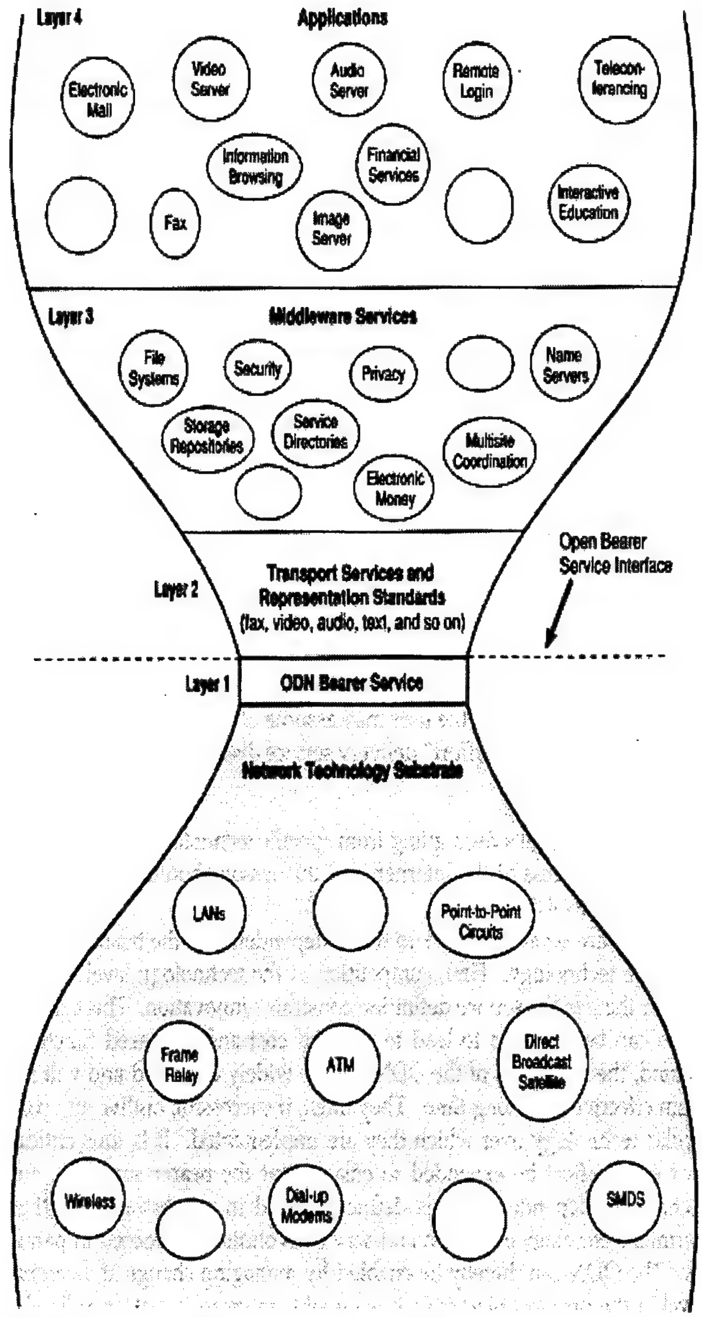

Figure 5.4 "Hourglass" figure illustrating the centrality of the open data networking (ODN) bearer service. From [NRC,94]

system, the postal service. The postal system's elemental unit of transfer is the letter, or parcel. In an IP network the elemental unit of transfer is the *datagram*. Each datagram contains both a header (information on the outside of the envelope) and a data payload (the information inside the envelope). The header includes the datagram's destination and source (return) addresses, which makes each datagram self-describing. This allows each datagram to be handled by the network independently of all other datagrams. Transferring a datagram across an internet is analogous to mailing a single letter through the postal system. A transmitting host "drops" a datagram into the network, and the network's routers forward the datagram according to its destination address. The actual route taken by each datagram is typically not known by the sender ahead of time. Intermediate routers are free to decide dynamically which route is best. If a sequence of datagrams is sent to the same recipient, each datagram may or may not traverse the same route through the network. This can cause unpredictable delay and/or out-of-order delivery. Although the network does not capriciously discard datagrams, at the internet layer there is no *guarantee* that any particular datagram will be delivered at all.

This connectionless method of communication contrasts sharply with that of connection-oriented services such as the public telephone network, Asynchronous Transfer Mode (ATM), and X.25 packet switching. Prior to transferring data across one of these connection-oriented networks, signaling must be used to establish a connection and negotiate a route with all intermediate switches between the end points. Once the connection is set up, all data flows over the same route. This ensures that data packets are delivered in order and with typically consistent delay. Furthermore, all of the intermediate switches in the route must be kept aware of the status of the connection between the endpoints. If a failure occurs at any point along the route, the connection is closed.

Despite some of the benefits of connection-oriented technologies, IP is more appropriate for the tactical internet. Being connectionless, IP is more robust in the presence of hostile and uncertain network conditions. If a communications link fails or

becomes heavily congested, IP routers are free to dynamically forward datagrams via better paths. Further, since IP does not use signaling to establish connections, it creates less overhead data traffic on the already bandwidth-constrained tactical communications circuits.

There are many requirements for network communications that were never intended to be met by IP alone. The internet layer protocol (IP) accomplishes host-to-host connectionless unreliable communication across disparate networks. Other important functions in data communications (such as error checking and correction) are performed by other protocols in the TCP/ IP suite. The next section describes how other protocols work together with IP to provide a greater range of services in the combined TCP/IP suite.

5. Connection-Oriented Services in a TCP/IP Internet

The Internet Protocol (IP) was designed to provide a simple network service for more complex end-system communications. Put another way most of the "intelligence" in a TCP/IP networkis in the end-systems rather than in the network infrastructure [Comer,95]. The TCP/IP protocol suite has two transport layer protocols that manage end-to-end communications: UDP and TCP. User Datagram Protocol (UDP) simply extends IP's connectionless datagram delivery service up to the applications layer. UDP adds no reliability, but does add the capability to deliver to a datagram directly to a specific *application* or *process* on the end-system (host). IP can only deliver datagrams to a destination *host*. [Comer,95]

The Transmission Control Protocol (TCP) provides reliable connection-oriented communications between two (and only two) applications. TCP also performs flow control to alleviate congestion in the network. TCP is a complex protocol, and a complete discussion of TCP is beyond the scope of this thesis. What follows is an overview of the features that TCP adds to IP's basic service.

An application invokes TCP to establish a communications connection with an application on another host. The application sends TCP a stream of data and TCP uses IP's delivery service to exchange packets with the TCP layer software on the destination host. TCP sequences packets so they can be put back in order after receipt. On the receiving end TCP performs error checking and sends positive packet acknowledgements (ACKs) back to the transmitter to confirm error free delivery. Unacknowledged packets are retransmitted after a timeout period. [Comer,95]

A form of flow control is also provided by TCP [Jacobson,94]. Flow control is necessary in a shared data network to avoid overloading switching nodes (routers) and disrupting service for all users. When TCP detects delays in receiving packet acknowledgements, it assumes that the cause is network congestion. To avoid causing further congestion TCP quickly "backs off" its sending rate and allows more time before retransmitting unacknowledged packets. Once congestion subsides TCP slowly increases its sending rate back to a normal level. This exponential back off and slow start procedure is effective in controlling congestion, but wreaks havoc on delay-sensitive data traffic such as audio and video streams. Workarounds for TCP are often necessary on wireless and satellite communications links where intermittent communications and propagation delay, rather than congestion, are the major causes of unacknowledged packets. [Comer,95]

C. IPV4 ADDRESSING

1. Overview of IPv4 Addressing Architecture

Addressing plays a vital role in the architecture of an IP-based internet. To permit any host to communicate with any other host in the internet, the architecture must define a common method of identifying each host. IP defines this identifier as the IP address. A datagram is routed through the network solely on the basis of its destination IP address. Without a proper and valid IP address, a datagram cannot be delivered to its

intended recipient. A host's IP address, therefore, indicates not only the host's **identity**, but also the host's topological **location** in the network.

Like a postal address or a telephone number, an IP address must be "globally" unique. In this context "global" is relative; it encompasses *all* computers and networks that are reachable by that IP internet. Address uniqueness ensures unambiguous handling of datagrams. Sharing of the same IP address by different locations in the network otherwise confuses routers as to where to deliver datagrams destined for that address. (Multicast addresses are the exception to this rule. IP Multicast is discussed in Section D of this chapter.) Technically, global address uniqueness is not always required. For example, a MEU might establish a TCP/IP network in support of a training exercise. If the MEU's tactical internet has no connection to any other IP network, then the MEU can assign arbitrary IP addresses that are at least unique within the MEU network. However, if the MEU's network connects to the NIPRNET, SIPRNET or the global Internet *at any point*, the MEU's addresses must be truly "globally" unique.

Uniqueness of addresses in the global Internet is ensured by having a single body, the Internet Network Information Center (InterNIC), vested with address assignment authority [InterNIC,96]. Any organization that wants to connect its network to that are to the global Internet must obtain IP network addresses from the InterNIC. Military networks numbers are obtained from InterNIC by the DoD Network Information Center [DISA,96b]. The DoD NIC in turn assigns IP addresses to the military services as necessary.

Many commercial businesses have installed private enterprise-wide TCP/IP networks called "intranets" [Cortese,96]. (Although the Marine Corps tactical internet fits the corporate definition of *intranet*, the military uses *intranet* in a data link layer context [MCCDC,95b]. To avoid confusion the term intranet is not used in this study.) Since many of the hosts in these private internets may never be connected to the global Internet, the Internet Engineering Task Force (IETF) recommended that private internets use non-globally unique IP addresses in order to help extend the life of IPv4 address

space [Rekhter,96a]. In conjunction with the IETF plan the Internet Assigned Numbers Authority (IANA) reserved several large blocks of IPv4 addresses for use by private internets. These addresses can be used by many organizations simultaneously so long as their networks are not connected to the Internet. An advantage of using the private IP address space is that it offers an organization many more addresses can be obtained from the globally unique address space. The main disadvantage is that any host or network that is subsequently connected to the Internet must be renumbered. [Rekhter,96b]

The Tactical Data Network will be connected to the SIPRNET and NIPRNET. It must be assumed that all hosts in the tactical internet will have access to these global DoD networks, as well as to the Internet. Therefore it is imperative that globally unique IP addresses be used within the Tactical Data Network (TDN).

2. IPv4 Address Format

IPv4 addresses are 32-bit binary numbers. As mentioned above, both identity and location is embedded in the address in order to facilitate more efficient network routing. Each IP address is actually a pair (*networkID, hostID*), where the *networkID* identifies a network and the *hostID* identifies a host attached to that network. Internet routers use only the *networkID* portion of the address to forward datagrams to the destination network. The router on the destination network uses the *hostID* portion of the address to forward the datagram to the destination host. [Comer,95]

a. IPv4 Address Classes

In order to support different sizes of networks, the total IPv4 address space (2^{32} addresses) was partitioned into five address classes (Figure 5.5). The first five bits of an address indicate its class. Class A, B, and C addresses differ in the number of the 32 bits that correspond to the *networkID*. For example, class B addresses allocate 14 bits to the *networkID* portion, and 16 bits to the *hostID* portion. This yields a total of 2^{14} (i.e., 16,382) possible class B networks, each of which can include up to 2^{16} (i.e., 65,534)

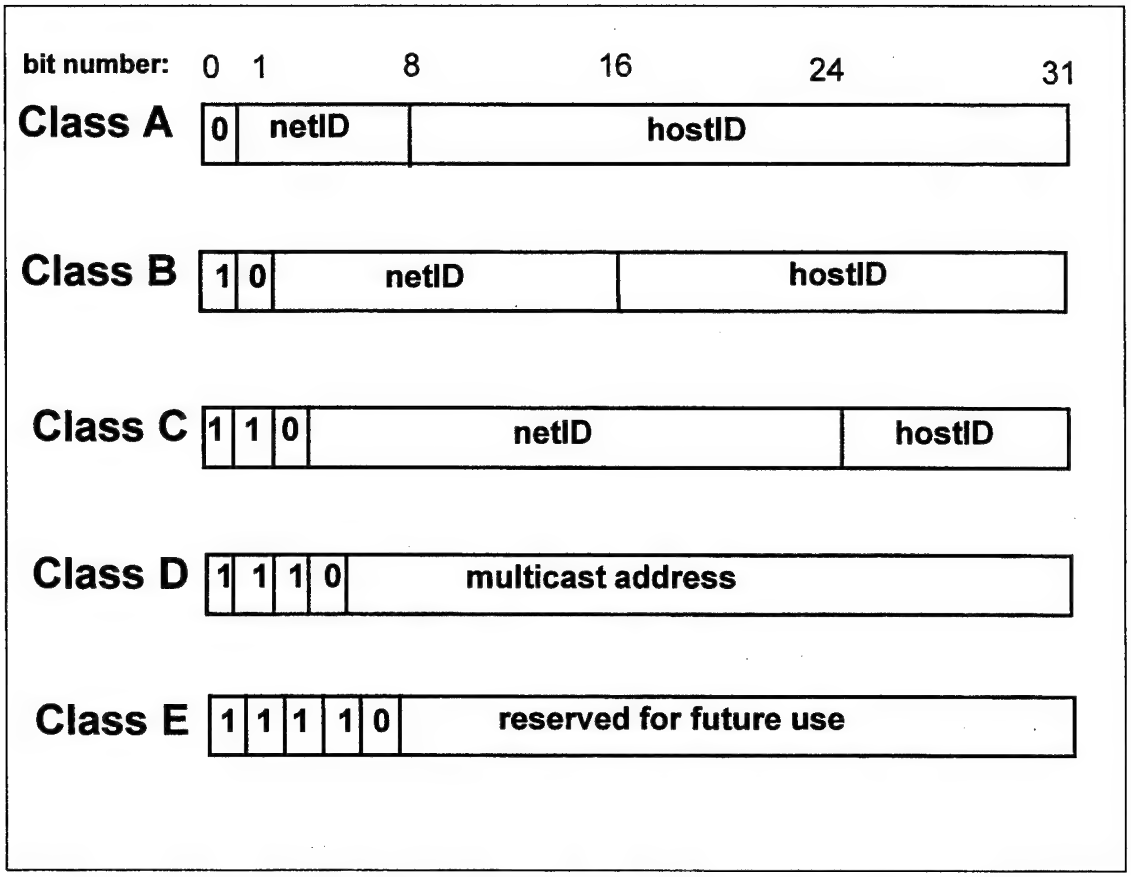

Figure 5.5 The five forms of IPv4 addresses. The numbers across the top (0-31) indicate the order of the bits. After [Comer,95]

hosts. Thus there are more than 2 million possible class C network numbers, each of which can support as many as 254 hosts (host#s 0 and 255 are reserved). [Comer,95]

The problem with this three-level class breakdown is that it does not efficiently support the intermediate size network partitions that are expected in the Marine Corps' tactical internet. The step sizes (256 and 65,534) between network classes is too great. *Subnetting* and *supernetting* were developed by the Internet community to alleviate this problem.

b. Subnetting

Subnetting is simply the further partitioning of the *hostID* portion of a standard class A, B, or C address into a *subnetworkID* and a *hostID*, as depicted in Figure 5.6. Subnetting permits several physical networks to share a single IP network number. Although it reduces the available address space slightly and can be tricky to set up properly, subnetting can improve throughput in some network topologies.

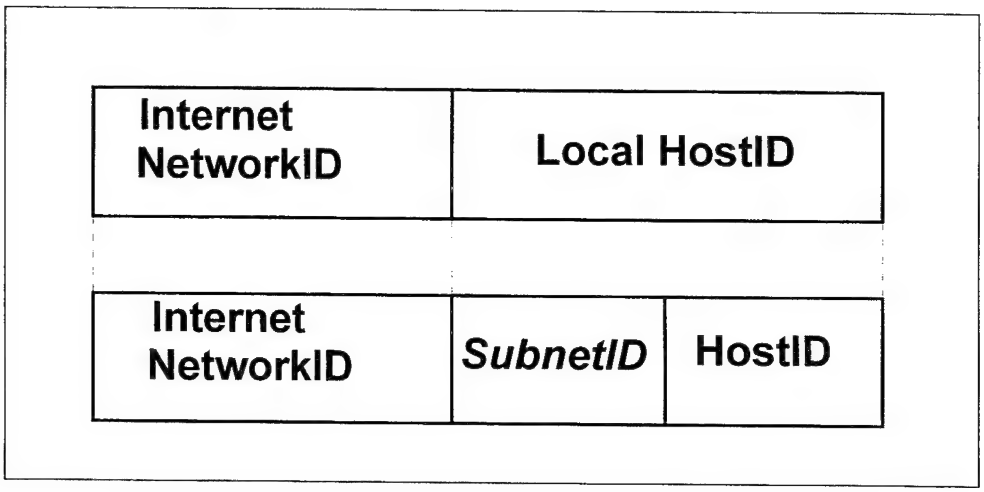

Figure 5.6 (a) Conceptual representation of 32-bit IP address in original class structure, and (b) using subnet scheme. After [Comer,95].

A simple example can illustrate subnetting in the tactical internet. In Figure 5.7 a unit has been assigned the class C network number *192.187.179.0.* There are actually four physical local-area network (LAN) segments connected to this unit's router. Consider what happens when a datagram containing the destination address *192.187.179.34* arrives at the router from somewhere in the internet. If subnetting is not used, the router has no way of knowing that the host identified by *192.187.179.34* is attached to LAN segment #1. The router must then broadcast the datagram on all four LAN segments. If instead each LAN segment is assigned a subnet number, the local router can directly determine the physical LAN segment to which a given destination

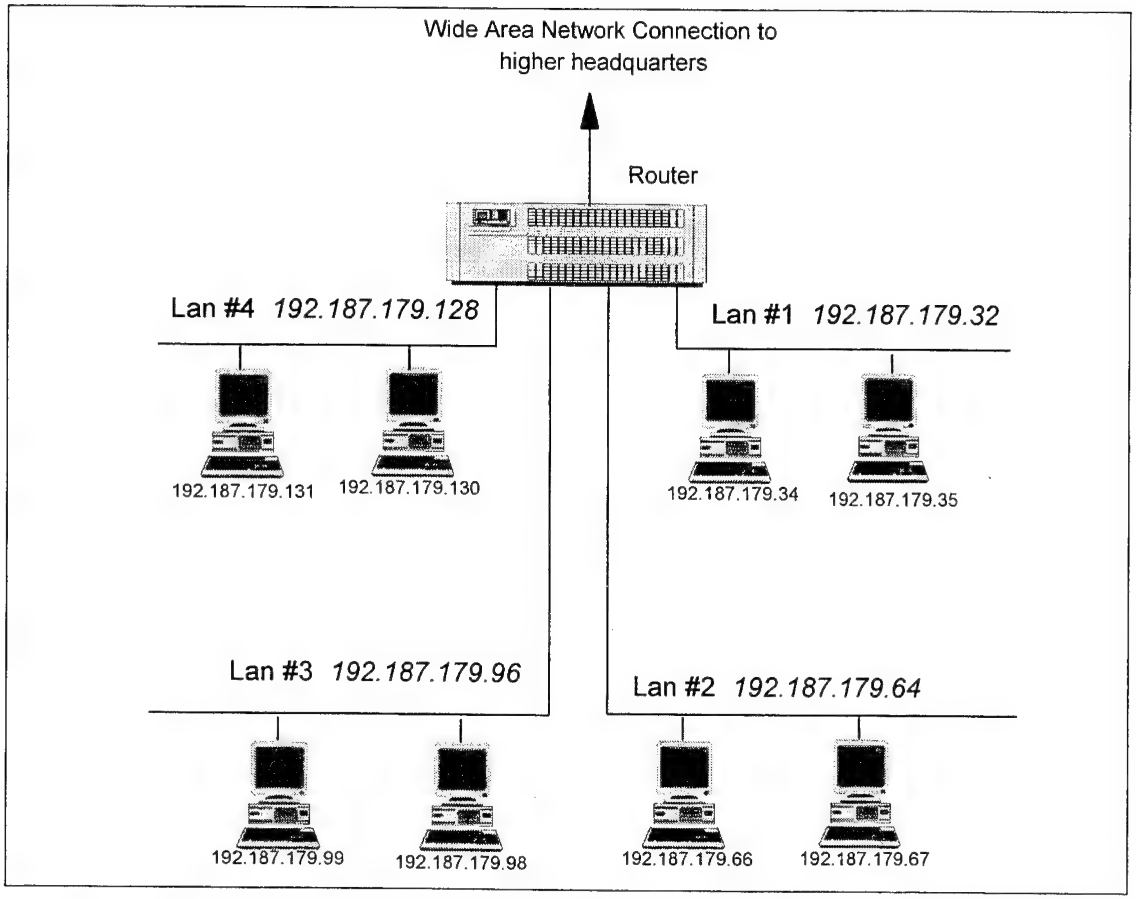

Figure 5.7 Example of a TDN subnet scheme within a regiment.

host is attached. For the example in Figure 5.7, the first three bits of the *hostID* portion of the class C address *192.187.179.0* were used as the *subnetworkID*. The resulting subnet numbering scheme breakdown is shown in Table 5.1. A datagram destined for host *192.187.179.66* (binary address: 11000000.10111011.10110011.**010**00010), for example, would be transmitted by the router only on LAN segment 2.

LAN seg	Subnet Number	Binary Subnet Number	Router Subnet Port Number	Range of host IDs
unused	192.187.179.0	11000000.10111011.10110011.**000**00000	192.187.179.1	2-30
1	192.187.179.32	11000000.10111011.10110011.**001**00000	192.187.179.33	34-62
2	192.187.179.64	11000000.10111011.10110011.**010**00000	192.187.179.65	66-94
3	192.187.179.96	11000000.10111011.10110011.**011**00000	192.187.179.97	98-126
4	192.187.179.128	11000000.10111011.10110011.**100**00000	192.187.179.129	130-158
unused	192.187.179.160	11000000.10111011.10110011.**101**00000	192.187.179.161	162-190
unused	192.187.179.192	11000000.10111011.10110011.**110**00000	192.187.179.193	194-222
unused	192.187.179.224	11000000.10111011.10110011.**111**00000	192.187.179.225	226-254

Table 5.1 Subnetting the Class C IP Address 192.187.179.0

In order to perform routing in the presence of subnetting, network routers must be able to distinguish which portion of the address corresponds to the *subnetworkID*. This is done by including a *subnet bit mask* in the routing table along with the IP address. All of the bits that are set to "1" indicate the *networkID* portion of the IP address, to which the subnet bit mask corresponds. An example of the bit mask is shown in Figure 5.8.

Subnetting is supported by most current routing protocols, including Open Shortest Path First version 2 (OSPFv2), Interior Gateway Routing Protocol (IGRP), and Border Gateway Protocol 4 (BGP-4). However, there are several drawbacks to subnetting. Subnet bit masks add to the information that routers must store in their routing tables. This may not be a major concern in the Marine Corps since TDN routing tables will probably be small anyway.

Subnetting also reduces the original address space by using address bits to indicate subnet hierarchy [WRQ,95]. Subnetting can reduce aggregate bandwidth requirements if traffic can be kept within each subnet. However, maintaining proper subnets is a challenging network administration task. In practice, subnetting is generally not advised. A further example demonstrating subnetting can be found in [Bigelow,95].

Subnet Address	192.187.179.64
Binary Subnet Address	11000000.10111011.10110011.0100000
Binary Bit Mask	11111111.11111111.11111111.11100000
Bit Mask	255.255.255.224

Figure 5.8 Example of Subnet Bit Mask.

c. Supernetting

Intermediate-size networks that do not have enough hosts to fully utilize a class B address, but do have more than enough for a class C address, have another addressing option: *supernetting*. Supernetting (also called *summarization)* is approximately the opposite of subnetting. Whereas subnetting takes bits from the *hostID* portion of the address and adds them to the *networkID* portion, supernetting takes bits from the *networkID* portion and adds them to the local *hostID* portion [NCCOSC,95]. The effect is to aggregate a number of class C network addresses into one larger network address. Only that one aggregated network number needs to be advertised throughout the internet routing system.

The tactical internet configuration depicted in Figure 5.9 can be used to illustrate how supernetting might benefit the Tactical Data Network. Suppose that there is a router at each battalion of the 6th Regiment, and that each of these routers can only access the rest of the tactical internet via the regiment's router. Notice that all of the battalions' class C addresses begin with ***11000000.10111011.10110****xxx.0* (binary format), which corresponds to *192.187.176.0* in dotted decimal format. Therefore, the only network number that needs to be advertised to the rest of the internet by the regiment's router is *192.187.176.0* (the supernet network address for these five networks). Routers *192.187.179.0* through *192.187.183.0* are handled uniquely by the boundary router *192.187.177.0*. The consolidation of network number advertisements

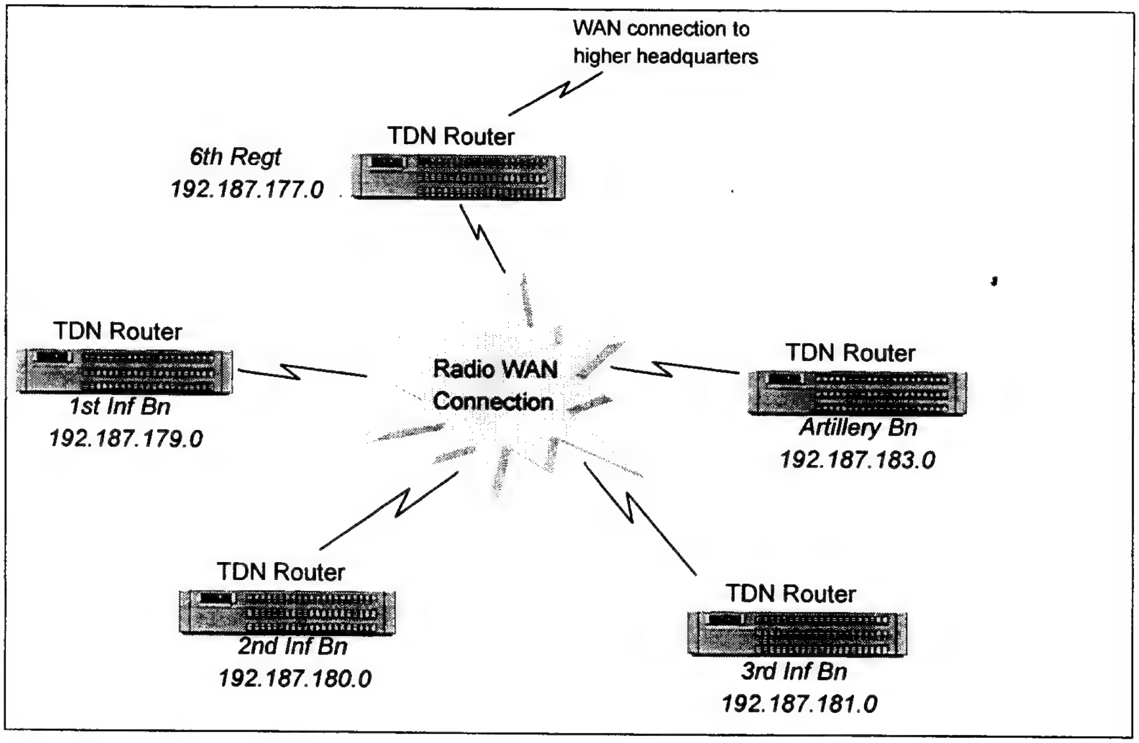

Figure 5.9 Notional regimental Tactical Data Network configuration.

between routers greatly reduces both the routing computation required the amount of bandwidth consumed for network overhead.

Notionally, all of the networks summarized by a supernet address must be reachable via a common gateway, or border router, that interfaces with the rest of the internet. In practice, if one of the battalion networks within the supernet splits off from the rest of the regiment, that battalion network advertises itself independently.. In routing tables these addresses appear as shown in Figure 5.10. Since the *networkID* portion of the separate network's address, identified by the bit mask, is longer than the *networkID* portion of the supernet address, routers will use the *longest match* to perform the routing function [Comer,95]. This allows both the efficiency of sparse routing overhead and the flexibility to relocate subnetworks according to mission requirements.

Supernet address:	*192.187.176.0*	11000000.10111011.10110000.00000000
Supernet bit mask:		11111111.11111111.11111000.00000000
Separate network addr:	*192.187.179.0*	11000000.10111011.10110011.00000000
Separate network bit mask:		11111111.11111111.11111111.00000000

Figure 5.10 Example routing table entries for the network in Figure 5.9 with 1st Bn advertised as a separate entry.

3. Classless Inter-Domain Routing (CIDR)

Subnetting and supernetting can be combined in an addressing and routing scheme called Classless Inter-Domain Routing (CIDR) [Fuller,93]. CIDR allows any portion of the 32-bit IP address to be allocated to the *networkID*. This scheme is classless because routers do not need to determine whether an address is class A, B, or C. Instead, the routers use the bit mask that accompanies the IP address to determine the *networkID* portion of the address. [Fuller,93]

CIDR has many advantages for tactical IP addressing. By breaking the subnet size restrictions of the original address class hierarchy, CIDR allows network managers greater flexibility and autonomy in defining an addressing and routing structure. CIDR may also enhance the interoperability of TDN. All of the routing protocols planned for use in NIPRNET and SIPRNET support CIDR, and the Navy is using CIDR as the basis for developing its own tactical IP addressing plan [NCCOSC,95].

4. Configuring an IP Address

Each host computer attached to a TCP/IP network must know its own IP address before it can send and receive datagrams. The host must also know the IP address of its local router, the correct subnet bit mask to use, and the IP address of a domain name server (name servers are discussed in the next section). A host obtains this information

from either its own disk memory or an address server on the network. In either case, the binding between the IP address and the host's network interface is normally *pre*configured manually. When the host moves to another subnet or gets a new network interface card, its IP address must also be *re*configured manually. The same procedures are required for adding any new host to a subnet. These requirements are problematic. In a dynamically changing network environment, such as in a field command center, frequent renumbering is an unsatisfactory and failure-prone burden on both the network administrator and the end user.

The Internet Engineering Task Force (IETF) developed the Dynamic Host Configuration Protocol (DHCP) to help alleviate this problem. The concept of DHCP is simple. A DHCP server(s) is placed on the network and entrusted with a set of IP addresses. When a host on the network boots up, it sends a configuration request out to the network. The DHCP server either picks up the request directly, or the host's local router relays the request to the nearest DHCP server. The DHCP server then issues the host an IP address for a specified lease period. The host must periodically renew the lease, or the DHCP reclaims the address. In practice, DHCP can support dynamic or static IP address configuration. [Wobus,96]

There are several problems with DHCP. The most obvious is that address configuration, which is necessary before a host can communicate over the network, is dependent upon the DHCP server. A host cannot work autonomously without the DHCP server, and the system (as currently defined) is not fault tolerant. If the DHCP server fails, hosts can neither obtain IP addresses nor renew leases on previously issued IP addresses [Murai,95]. This failure might bring down an entire portion of the network. It must also be noted that DHCP is not yet a mature protocol. DHCP is currently defined as a *Proposed Internet Standard* (the Internet standards process is described in Chapter VII), and solutions to many of these problems are currently being pursued by the IETF [Wobus,96].

5. Domain Name System (DNS)

IP addresses are not user friendly. They are designed to be used by machines, not people. Further, IP addresses are not necessarily permanent since computer network topologies can change. Thus it may be difficult to find out the current IP address of a destination host. Domain names are abstractions of IP addresses that were created to give users and application programs a more intuitive, durable method of referring to hosts and host network interfaces. Domain names such as *www.usmc.mil* (the name of the Marine Corps' World Wide Web site) have no implicit meaning to the network infrastructure. To be useful in networking, domain names must be mapped to an IP address.[Comer,95]

The domain name system (DNS) is a set of distributed databases called *name servers* that work together to map (or resolve) domain names to IP addresses [Comer,95]. For example, an application passes the domain name of the destination host with which it wants to communicate to the DNS client software running on the local host. The DNS client coordinates with the system of DNS name servers to obtain the corresponding IP address of the destination host. The IP address is then used by the host machines for all communications. Thus establishment of a proper and robust DNS is a crucial requirement of the tactical internet. The actual implementation of DNS in the Tactical Data Network is not a focus of this study. DNS is mentioned here for completeness, and to illustrate how IP addresses are used by end user systems. DNS will be discussed briefly again in Section D, which deals with IPv4 support for mobile computing.

6. Summary of IPv4 Addressing

The complexities and pitfalls of IP addressing are legion. This stresses the need for a sound tactical IP addressing architecture. Tactical IP addressing plans must accommodate a wide variety of command post network topologies that may be constantly changing. Since topology is embedded in the IP address, adapting to these types of changes is too daunting a task for manual network management methods. Dynamic

addressing protocols are necessary to ensure that end users have transparent and error-free interface to the internet.

A full case study of building IP-based local-area networks (LANs) to create a wide-area network (WAN) is available online in [Bigelow,95]. A detailed analysis of network management considerations for LANs in a combined WAN appears in [Trepanier,95].

D. IP MULTICAST

1. Overview

Multicasting is required in tactical internetworking. This section is a brief overview of the multicast capabilities of the current Internet Protocol (IPv4) and how multicasting is used in the global Internet. The following section considers issues related to multicasting with IPv4 in the tactical environment.

a. Unicast/Broadcast/Multicast

There are three fundamental types of IPv4 address: *unicast, broadcast*, and *multicast*. A unicast address is designed to transmit a datagram to a *single* destination. A broadcast address is designed to deliver a datagram to *every host* on the destination local-area network. A multicast address enables the delivery of a datagram to a *specific set of hosts*, called a *multicast group*, each of which may be physically located anywhere within an internet. IPv4 support for handling multicast datagrams is called IP Multicast. [Comer,95]

IP multicast group membership is dynamic. Any host with appropriate multicast-capable software can establish a multicast group, also called a *session*, by obtaining a multicast address and then announcing the group address and lifetime to the internet. Hosts are free to join or leave multicast sessions at any time, and a single host can be a member of many multicast groups simultaneously. A host does not have to be a member of a particular group to send traffic to that group (although membership is

recommended). When the number of members in a multicast group drops to zero, the group is effectively disbanded and the multicast address is freed for reuse. [Macedonia/Brutzman, 94]

b. Multicast in the Global Internet

The preponderance of data traffic on the global Internet is unicast. Browsing the Web is an example of unicast communication. A single client host running a Web browser typically establishes a communications connection with a single host running Web server software. Individual queries from Web browsers communicate with only one Web server at a time. In general, any application that employs TCP as a transport layer protocol is unicast. TCP is connection-oriented, and does not support multicast.

Because unicast traffic has predominated Internet usage, unicast Internet protocols are more mature than multicast protocols. However, interest in multicast is steadily developing. Multicast support for transmission of audio and video is now one of the most active areas of research in the Internet community. The Multicast Backbone (MBone) is one of the most successful applications of multicast technology in the global Internet and an example of dramatic results that can be produced by group research efforts.

MBone is a virtual IP Multicast network testbed that is layered on top of the existing physical topology of the Internet. Since many of the routers in the global Internet do not support IP Multicast, MBone is fragmented into islands of IP multicast-capable networks. Isolated multicast routers (mrouters) communicate with each other using a communications technique is known as "tunneling." The mrouters encapsulate the IP Multicast datagrams within regular unicast IP datagrams, then forward them through the portion of the Internet that does not support native multicast. Modern mrouters can communicate via native distribution of multicast traffic, without encapsulation or tunneling. [Macedonia/Brutzman,94]

MBone has existed since 1992. Thus far is has been used primarily to transmit audio and video from research conferences, IETF meetings, and special events such as space shuttle launches. The MBone can also be used for distance learning [Emswiler,95]. The MBone community has developed multicast protocols, as well as freely available multimedia applications compatible with nearly every computing platform on the market today [Kumar,96a].

Development of multicast protocols and applications continues to progress at a rapid rate. One recent proposal that may have direct application in the tactical internet is the use of Global Positioning System (GPS) data to determine IP addressing and routing [Imielinski,96]. GPS coordinates can be used to define a multicast group such that only tactical nodes within the geographical area bounded by the coordinates receive the multicast messages. The geographic region targeted for the multicast can be described numerically or by a line traced on an electronic map display. Mobile users can use GPS data to determine the correct multicast group to join for the area in which they are currently operating. This type of GPS-determined addressing and routing might greatly enhance the ease-of-use, security and scope control of tactical multicast. The proposed GPS-based protocols are in the early stage of definition. Nonetheless, the Marine Corps must track this development effort and determine what the role of GPS in the tactical internet can be.

2. Multicast in the Tactical Environment

As mentioned in Chapter III, multicast has significant advantages over unicast for use in tactical communications. Multicast takes advantage of the inherent multicast/broadcast nature of physical media used in tactical communications, such as single channel radio, wireless LAN and Ethernet LAN. Compared to unicast, multicast uses less bandwidth and incurs less transmission delay. Although broadcasting also delivers data to multiple recipients at once, it wastes bandwidth and end-system computational power doing so. Furthermore, broadcast is not supportable past the

boundaries of individual LANs. Unlike broadcast, multicast allows the recipient to *select* which traffic is received. The selection is performed at the physical (hardware) network interface level. The network interface only listens to certain subscribed multicast addresses and passes only those data packets to the higher layer software. This keeps the CPU from being consumed by constantly sorting out which data to keep. By contrast, broadcast consumes excess CPU time because broadcast packets must be inspected by the higher layer software. [Macedonia/Brutzman,94]

Multicast fits closely with the "warrior pull" concept which is integral to the *C4I for the Warrior* (C4IFTW) vision. Under C4IFTW, the warrior decides which information is relevant to his mission and his battlespace, and chooses to pull (or receive) only that information. [Joint Staff,93]

In fact there are so many advantages to the use of multicast one researcher has described unicast as merely a special case of multicast in which the group consists of two end users [Symington,96]. Given the importance of multicast, there are six potential problems with using IP Multicast in the Tactical Data Network (TDN) that must be considered:

- Multicast address assignment/allocation
- Prompt termination of multicast sessions
- Determination of the appropriate scope of multicast sessions
- The optional nature of multicast support in commercial router implementations
- Dissemination of Direct Broadcast System (DBS) traffic
- Reliability of data transfer

a. Multicast Address Allocation

IP Multicast has no built-in address allocation mechanism. Multicast (Class D) IP addresses are dynamically obtained through protocol mechanisms within the multicast *application* programs themselves [Braudes,93]. Thus far, address duplication has not been a problem in the global Internet. There are few applications that manage multicast

sessions, and the multicast address space is huge (2^{28} possible addresses). As the Marine Corps and the other military services develop new multicast applications for tactical use, however, they must adopt some consistent means of obtaining and managing multicast addresses. Current applications and protocols appear adequate for this task [Handley,95].

If Class D addresses are dynamically assigned, there is no way to know a multicast group's address before the first group member announces it electronically to the network. All other hosts must wait passively until they receive the announcement, then those that want to join the group do so by notifying their local multicast routers. Depending on the topological scope of the multicast session, excessively distant users may not even receive the announcement of the group. This current method of joining an IP Multicast group is analogous to using a radio frequency scanner to locate the tactical C^2 radio net that you want to join. Passive procedures such as this do not fit with the changing nature of tactical network topology and the users' needs to rapidly exchange and distribute information. In order to make IP Multicast work in the tactical internet, it may be necessary to assign well-known, semi-permanent multicast addresses to high priority groups, and also to multicast groups that develop naturally from doctrinal command structure. Such an approach is gaining acceptance [Handley,95]. A detailed analysis of multicast address allocation and partitioning schemes appears in [Macedonia,95].

b. Termination of Multicast Sessions

Termination of host and subnetwork participation in a multicast group is also done passively. The local multicast routers (mrouters) are responsible for determining whether any local hosts are still members of any active multicast groups. The mrouters do so by periodically polling their multicast "constituents." If at least one local host claims membership in a multicast group, an mrouter must continue to forward traffic for that group. If after several polls no host claims membership in a particular multicast group, the local mrouter will notify all other mrouters to stop sending it traffic for that

multicast group. In the meantime, multicast data may be needlessly transmitted across tactical communications links. IPv4 Multicast currently lacks a globally employed protocol that allows hosts and mrouters to actively prune uninterested hosts and subnets from the multicast "tree." However, this is an active area of research and numerous developmental implementations exist [Voigt,96].

c. Scoping a Multicast Session

To preclude inundating the entire internet with multicast traffic that are only of local interest, IP Multicast provides a method for limiting the scope of multicast datagrams. The scope is a rough measure for the portion of the internet through which a multicast datagram is allowed to propagate. The scope of IP multicast is controlled by setting the Time-to-Live (TTL) field in each multicast IP datagram. Each time the datagram passes through a router, its TTL field is decremented (either by one, or by a preset bounding value such as 16 or 32). The router may also decrement the TTL by the number of seconds the datagram remain in the router's queue. When the TTL reaches zero, the datagram is discarded by the network.

Determining the proper TTL for tactical multicast may be difficult. It may be possible to guess the number of routers a datagram must pass through, but the delay in the tactical internet is likely to be unpredictable. TTL scoping is inherently crude and more precise mechanisms such as *pruning*, *grafting*, and *fast leave/join* are needed.

d. Universal Support for Multicast

In the global Internet, multicast has not been universally supported by routers or host operating systems. The result has been scattered islands of multicast networks (MBone) separated by unicast-only routers. A similarly awkward topology will emerge in the joint tactical internet architecture if multicast protocol support is not uniformly and universally adopted by all services. The Navy, for one, has ensured that all of its shipboard IP router implementations support multicast [NCCOSC,95]. In order to take full advantage of multicast capabilities, however, support must go beyond the network

infrastructure and the internet protocol layer. End-user applications, transport layer protocols, and internet protocols must implement multicast in an integrated fashion. Network interface cards must support multicast in hardware to prevent computational overload. Finally, software applications being developed for tactical data systems must extend their sole reliance on TCP, a unicast-only transport protocol, by incorporating multicast approaches.

e. Multicast Over the Global Broadcast Service (GBS)

GBS has become a high priority developmental program. GBS will have the capability to downlink high bandwidth (currently 23 Mbps) data streams to small earth stations receivers with 18-inch antennas. It is envisioned that GBS will transport the bulk of high-bandwidth data traffic being transmitted into a joint tactical area of operations. However, GBS is a one-way communications system with no direct return channel, and it remains to be seen whether IP can be used effectively with such a system. Most of the IP routing and multicast protocols require periodic router-router communications. There is research being done in this area by both military and commercial organizations [Starburst,96].

f. Reliable Multicast

Current implementations of IP Multicast are inherently unreliable. The Internet Protocol itself provides connectionless, unreliable datagram delivery. To get reliable (i.e. error-free and in-order) data transfer across an IP network, most applications use TCP. TCP does not support multicast. Multicast applications using the Internet employ the connectionless User Datagram Protocol (UDP) at the transport layer, and settle for unreliable delivery service from the network. This has worked for MBone applications because the nature of the audio and video traffic does not demand reliability. Transfer of essential high-volume data, such as Defense Messaging System (DMS) electronic mail, however, must be **both reliable and multicast**. IP must be capable of supporting both reliable and unreliable (best effort) data transfer. Rather than changing IP to make it

reliable, the Internet community is pursuing solutions to provide reliable multicast at the transport protocol layer.

The essential problem with both TCP and UDP is an all-or-nothing approach. TCP is completely reliable. UDP is completely unguaranteed. The level of reliability is currently driven by the protocol and network contention, not the user's requirement [Weaver,94]. Several reliable multicast transport layer protocols are in developmental or experimental stages. Much of the research in this area has centered on the scalability problems of reliable multicast in the global Internet. The basic problem with reliability is that lost data packets can cause a cascade of negative acknowledgement (NAK) messages, which in turn may reduce throughput further. This difficulty is referred to as the "NAK implosion" problem. Example application-based reliable multicast solutions that exist today include whiteboard (wb), in which updates are reliably transmitted from host to host , and the reliable audio tool (rat) which incorporates redundancy (i.e. forward error correction) to minimize the impact of lost audio packets [Floyd,95]. An alternative transport-layer protocol that provides selectable-reliability multicast is the Xpress Transport Protocol (XTP) [Weaver,94]. The basic challenge in all these approaches is to find appropriate tradeoffs between reliability and scalable throughput. It is likely that one or more of these protocols, once they are fully developed, will surely meet the reliable multicast needs of the Marine Corps tactical internet.

3. Multicast Summary

The multicast capability of IPv4 is adequate to meet the needs of the Marine Corps Tactical Data Network. However, there are several key aspects of IP Multicast that must be properly administered when implementing it in TDN. An appropriate multicast address allocation mechanism must be employed, and multicast sessions must be properly scoped and promptly terminated. Multicast support must be implemented throughout the TDN. Finally, appropriate balances between reliability and throughput must be achieved for multicast applications.

E. MOBILITY

1. Mobility Introduction

IPv4 currently provides no explicit support for mobility. The Internet Protocol was designed under the assumptions that each end system (host computer) and router has only one point of attachment to the network, and that each point of attachment changes infrequently or not at all [Perkins,96b]. To facilitate efficient routing in such a static network configuration, the IPv4 address represents both the destination node's **identity** and **location** (point of attachment). By hardwiring topological significance into IP addresses, the original Internet architecture severely restricted IP's ability to cope with mobile users and networks.

In the context of this study, mobility is really *mobile computing*. Mobile computing can be defined as using a computing device with a wired or wireless interface at different locations that cannot be accurately predicted by the network ahead of time [Ghosh,93]. It was noted in the previous chapter that the Tactical Data Network (TDN) will be required to support both mobile and non-mobile users. There is a significant trend toward mobile computing in commercial community as well. This has caused the IETF to accelerate its effort to develop mobility support within the TCP/IP protocol suite [Hinden, 95].

2. The Mobility Problem

The mobility challenge in the tactical internet is to allow end users, wherever they are in the battlespace, to access network services. Examples of mobile computing in the tactical internet were given in the previous chapter. Mobile nodes may maintain communication with the network while actually on the move (roaming), or they may disconnect from the internet in one place and reconnect in another. The mobile node can be an individual foot-mobile Marine carrying a single computing device or an entire

command center LAN being displaced. The network must have a means of forwarding datagrams to the relocated mobile user no matter where he is located or connected.

It is important to distinguish between *intra-network* and *inter-network* mobility. Intra-network mobility includes users who move about but remain physically connected to their home network either by radio, dial-up telephone or wireless LAN. Mobility of this type is usually handled by data link (network interface) layer protocols, such as MIL-STD-188-220A (tactical radio) and IEEE 802.11 (wireless LAN) [MCCDC,95b]. Inter-network mobility entails a user changing the physical network through which he accesses the internet. Inter-network mobility must be accommodated by the Internet Protocol suite.

There are several approaches to solving the inter-network mobility problem. These can be simply summarized as:

1. Broadcast packets for all mobile users to every subnetwork within the tactical internet.

2. Send all packets for all mobile users to a "mobile node" multicast group.

3. Have the mobile user change his IP address each time he moves to a new network.

4. Have the mobile user retain the same IP address no matter where he is in the network.

5. Have the mobile user maintain an up-to-date "care-of" address and have his home network forward his data traffic.

The broadcast approach can be ruled out for the same reasons stated in the multicast section: wasted bandwidth and processing time. The advantage of the multicast option is its simplicity of concept. When a node "goes mobile" it joins the multicast group and will receive its traffic regardless of its point of network attachment. A drawback to this approach is that reliability and bandwidth may not scale well. A mobile multicast group

with a large number of members is essentially a *broadcast* group from the individual mobile node's perspective. Thus a multicast approach can overwhelm the low-bandwidth wireless communications links typically used by mobile nodes.

Another drawback to the mobile multicast approach is that the network must keep track of which specific nodes are members of the multicast group. This is fundamentally different from the way IP multicast works. IP multicast routers only keep track of whether *any* members of a multicast group reside on a destination LAN, not which specific hosts are members [Deering,89]. This problem can be rectified by assigning each mobile node a unique multicast address, but such an approach complicates multicast routing and does not scale well for point-to-point communications. Finally, mobile nodes may be limited in their use of applications because IP multicast does not support reliable data transfer.

The third approach of having mobile nodes change IP addresses requires two things of the network: a method of assigning a temporary address to each mobile user for each network to which he attaches, and a method of dynamically updating the domain name System (DNS) to ensure correct binding of the end user's domain name to the current temporary IP address. A temporary address assignment method already exists: the Dynamic Host Configuration Protocol (DHCP) discussed in the *IP Addressing* section above. However, a open systems standard for DHCP-to-DNS communications has not been established. Nor does a standard method exist within DNS to dynamically update IP address-to-domain name bindings. The Army uses the dynamic address-to-domain name approach to connect mobile data users to its Mobile Subscriber Equipment (MSE) network. The Army Tactical Name Server (TNS) solves the dynamic DNS binding problem by employing a proprietary protocol [Spector,96]. Open systems solutions to the issue are being actively pursued by the IETF, and several protocol specifications are currently in draft form [Droms,96].

The strength of the DHCP approach is that the mobile end user maintains only one logical point of attachment to the internet. Thus DHCP routing can be kept optimal. One

of the weaknesses of this method is that it relies on both the DHCP server and the DNS name server to make the system work. A second weakness is that this approach requires every affected portion of the internet to implement mobility support protocols.

The fourth approach whereby the mobile node retains a "permanent" IP address places the entire burden of maintaining mobile user connectivity on the internet's routers. If a mobile node is identified by an unchanging IP address regardless of where it is physically connected to the network, the *networkID* (location) portion of the node's IP address is of no use in routing. To compensate for this loss of functionality, the routers must maintain a *host-specific route* for every mobile node in their routing tables. Unfortunately, large numbers of dynamically changing host-specific routes can lead to routing instability, and can limit the expandability of the network. The strengths of host-specific routes are that DNS bindings remain stable and that no reconfiguration or readdressing is necessary at the end-user level. The IETF rejected this solution because it cannot efficiently scale to the global Internet. Therefore, the feasibility of permanent addressing for TDN is unlikely.

The care-of address approach is a hybrid of the previous two. The Mobile IP Working Group of the IETF has proposed a mobility support extension for IP that essentially implements the "mail forwarding" concept. This protocol extension (called *Mobile IP*) is discussed in detail in the next section.

3. The IETF Solution: Mobile IP

The Mobile IP proposal was released as an Internet Draft in February 1996 [Perkins,96b]. It is still immature and has not been field tested. Nonetheless, this proposal indicates the direction in which the Internet community is moving to provide support for mobile computing.

Mobile IP has several basic design principles:

- A mobile node must not have to change its IP address.

- A mobile node must be able to communicate with other nodes that do not implement Mobile IP.
- Mobile IP must work without requiring implementation of mobility support throughout the entire network infrastructure.
- All messages regarding the location of a mobile node must be authenticated.

Mobile IP assumes that every mobile node has a *home network*. The home network is the node's usual point of attachment to the internet. For example, a battalion commander's C^2 vehicle might be considered a mobile node whose home network is the battalion's Tactical Data Network. Any other network to which a mobile node is currently attached is called a *visited* or *foreign network*. Each mobile node is issued a "permanent" IP address on its home network. The fundamental concept of Mobile IP is illustrated in Figure 5.11. When a mobile node is away from its home network, the mobile node uses a *care-of address*. The mobile node uses its home IP address when sending datagrams. Replies and incoming datagrams are also sent to that home IP address. The incoming traffic is intercepted by a mobility-capabable router, called the *home agent,* on the mobile node's home network. The traffice is then forwarded to the mobile node's current care-of address.

This description of Mobile IP is greatly simplified, and due to a variety of other considerations the actual protocol remains quite complex. A mobile node may or may not make use of a *foreign agent.* A foreign agent is a router on a visited network that acts as a surrogate for the mobile node. Once the mobile node registers its presence with the foreign agent, the foreign agent performs all coordination with the appropriate home agent. The home agent tunnels the mobile node's incoming datagrams to the foreign agent's IP address. The foreign agent then delivers those datagrams to the mobile node via a local physical network connection.

A network's foreign agent can support many mobile nodes. Therefore employing foreign agents eliminates the need to assign temporary IP address to visiting mobile

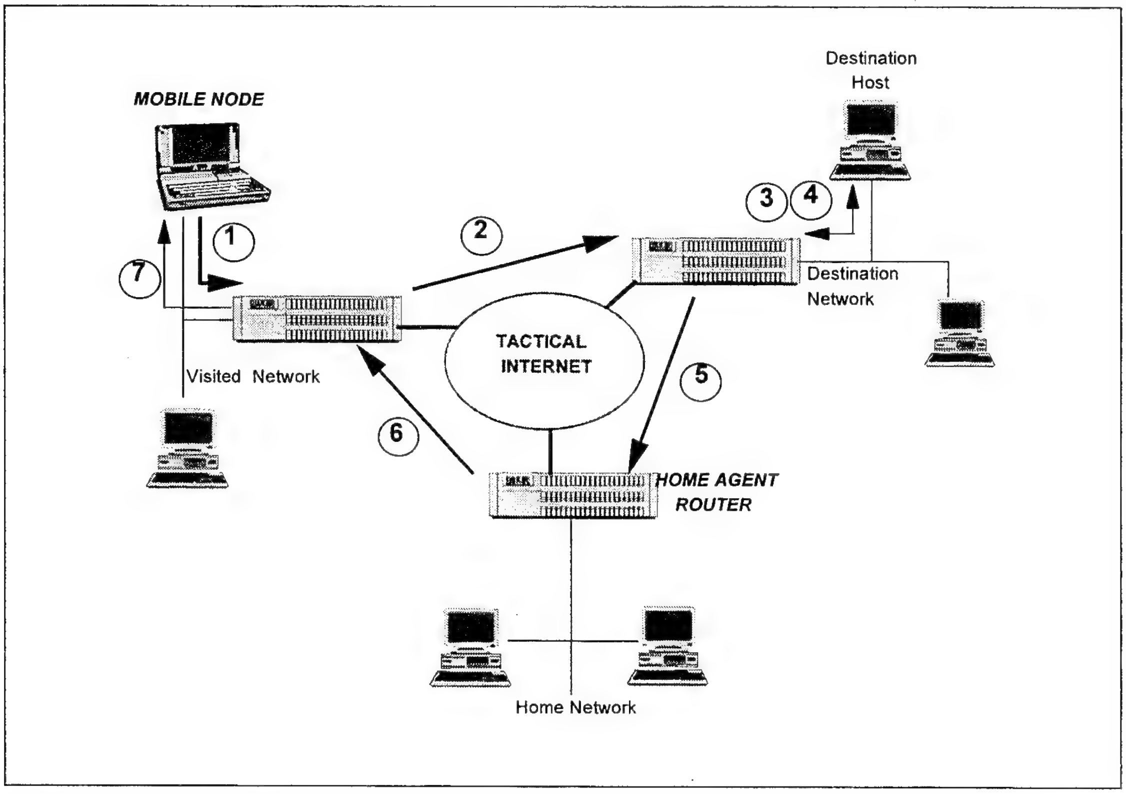

Figure 5.11 The Concept of Mobile IP. (1) A mobile node attached to a visited network sends a datagram to the destination host using the mobile node's home network IP address as the source address of the datagram. (2) The datagram is routed through the network as usual. (3) The destination host receives the datagram, and (4) sends a reply to the source IP address. (5) The reply is routed by the internet to the source IP address, i.e. the mobile node's home network. (6) The home agent intercepts the reply and forwards it to the mobile node's current care-of address (7) on the current visited network. Mobile node routing and home-agent router updates are handled separately. [Perkins, 96b]

nodes. This is the major benefit of foreign agents. The major advantage of not using the foreign agent approach is that communications are not dependent on the presence of a foreign agent on every visited network. Mobile IP allows both methods to be used together in the same network. [Perkins,96b]

Mobile IP provides an elegant solution for the type of mobility that is emerging in the commercial world. It also appears to meet many of the Marine Corps' end user mobility needs as well. However it falls short in one respect: the necessity of the home agent. The type of mobile node envisioned by Mobile IP is a laptop/palmtop computer that is moved from office to office, or office to hotel room, reconnecting to the Internet

at each location. There is an implicit assumption that the node's home network (and home agent) remains on-line at all times. In the expeditionary tactical environment of the Marine Corps' TDN, continuous home-agent availability is not a valid assumption. Tactical command centers displace frequently. The command center's data network is normally unavailable during these displacements. Under the Mobile IP plan, a mobile node that was away from its home network during a displacement would be unable to communicate with the rest of the internet. Thus extensions to this approach in terms of procedures and protocols will likely be needed to support TDN requirements.

4. Mobility Summary

Overall, Mobile IP appears to be a well-thought-out protocol. It remains to be seen how it will mature and be implemented in real-world systems. All of the proposed solutions for mobility mentioned here are bound to have problems. They are attempts to stretch the limits of IP to support a networking environment for which it was not originally intended. All these proposals, and new ones that may yet be developed, will need to be tested to determine which best meets the mobility needs of the Marine Corps.

F. IPV4 SUPPORT FOR QUALITY OF SERVICE (QOS)

1. QoS Introduction

The basic quality of service delivered by IPv4 at the internet layer is classified as "best effort." Any datagram handled by the IP layer will be delivered to its destination as soon as possible, but with no specific commitment as to bandwidth, delay or absolute reliability [Bradner,96a]. Using TCP over IPv4 guarantees end-to-end reliability (a part of QoS) but without other guarantees. Therefore, IPv4 does not offer true quality of service guarantees. This can be a problem for applications that need to communicate in real time.

2. Real-Time Data

Real-time data traffic (such as audio and video) has a time-sequence structure that must be maintained during transmission or restored after transmission. When real-time data is transmitted over a shared network infrastructure like an IP internet, the time structure of the data can become distorted by the delays induced by intermediate switching nodes (routers) [Jacobson,94]. Competition among data traffic from different sources creates variable length queues at intermediate internet routers. These router queuing delays can get translated into variable delays in end-to-end delivery of the real-time data [Braden,94]. To some extent applications can compensate for variable delay by buffering incoming real-time data, recovering the time sequence of the data packets, and then playing out the data with reconstructed timing [Jacobson,94]. Forward error correction can also ameliorate loss problems [Brutzman,95]. Nonetheless, the amount of delay that can be buffered by end-system applications is limited by memory size and user latencies. Thus the network must be able to bound the delay [Braden,94].

3. QoS Guarantees

In order to offer quality of service guarantees the network infrastructure must have at least three features:

- a means to identify the bits that require special handling.
- a means to reserve resources across the network in order to make good on the guarantee.
- a means for applications to negotiate QoS guarantees across the network.

None of these capabilities are built into IPv4. TCP does have a *type-of-service* field, which is a primitive quality of service, but it is inadequate for real-time applications. TCP is strictly an end-to-end protocol that cannot control the intermediate network infrastructure devices.

The Internet community has made a number of proposals to create QoS features as add-ons to IPv4. The Reservation Setup Protocol (RSVP) and Stream Protocol 2 (ST-II)

are two experimental resource reservation protocols that have been in use for several years [Braden,94]. There are other protocols being worked on that will allow different qualities of service for different recipients of the same multicast data. Yet another working group is developing QoS negotiation methods that apply across wide-area networks (WANs) comprised of a mix of IP and ATM infrastructure [Borden,95]. Nevertheless these efforts are still experimental and commercial implementations might not occur until IP version 6 is ready for deployment.

G. SECURITY

1. Security Overview

Security is not a strong point of IPv4. Many of the global Internet's security vulnerabilities are inherent in the original protocol design. There are no security features built into IPv4 itself, and the few security features that do exist in other TCP/IP protocols are weak. Devices have been developed, however, that add security to TCP/IP networks.

The most popular Internet security mechanism is commonly referred to as a *firewall*. Firewalls are designed to keep unwanted and unauthorized traffic from the global Internet out of a private network, yet still allow the private network's users to access Internet services. Most firewalls are merely routers that filter incoming datagrams based upon the datagrams source address, destination address, higher level protocol, or other criteria specified by the private network's security manager. More sophisticated firewalls employ a proxy server, also called a bastion host. The bastion host prevents direct access to Internet services by the private network's users (it acts as their proxy) while filtering out unauthorized incoming Internet traffic. [Bruno, 96]

2. Authentication

As mentioned in Chapter IV there are three prime security concerns for internetworked applications: authentication, confidentiality and integrity. Most security features that do exist in the TCP/IP protocols are authentication mechanisms.

Unfortunately the form of authentication most often used is based on insecure IP addresses or (worse yet) domain names. These authentication techniques are easy to defeat [Bradner,96a]. A common method of attack called *spoofing* involves imitating the IP address of a "trusted" host or router in order to gain access to protected information resources. One avenue for a spoofing attack is to exploit a feature in IPv4 known as *source routing*. IPv4 will allow the originator of a datagram to specify certain (or all) intermediate routers that the datagram must pass through on its way to the destination address. The destination router must send reply datagrams back through the same intermediate routers. By carefully constructing the source route, an attacker can imitate any combination of hosts or routers in the network, thus defeating an address-based or domain-name-based authentication scheme. Authentication security was a prime consideration in the development of the Internet Protocol Security Architecture (IPSEC) discussed in Section 5 [Atkinson,95].

3. Confidentiality

There is some support for confidentiality at the IP layer. For example, the Motorola Network Encryption System (NES)™ provides datagram encryption but it does so in a manner that seals off the protected network from the rest of the internet [NCCOSC,95]. All of the military services plan to use NES (or some similar device) in the near term to provide IP network security for the different levels of classified data [JIEO,95a]. Unacceptable current drawbacks to NES are an elaborate configuration scheme, low bandwidth, and lack of support for IP Multicast. Additionally, security for the TDN must not be tied to one commercial vendor. Open systems security solutions are needed to ensure an evolutionary upgrade path for TDN security features.

4. Integrity

Some measure of data integrity is provided by the TCP/IP transport layer protocols (TCP and UDP) which can perform error detection using checksums [NCCOSC,95]. In a sophisticated information warfare environment, simple checksums

are inadequate. True integrity assurance is obtained through the use of electronically signed message digests, which are not currently part of the IPv4 protocol suite [Russell,91]. Prototype integrity mechanisms are among the security features for IPv4 (and also incorporated into IPv6) that have been produced by the IETF IPSEC Working Group [Atkinson,95].

5. Internet Protocol Security Architecture (IPSEC)

Recognizing the need for greater security support within the Internet Protocol, the Security Working Group of the IETF published a proposed standard IP security architecture in 1995. The IPSEC is intended to be implemented as an option with IPv4 and as an extension header in IPv6 (IPv6 security is discussed in the next chapter). [Atkinson,95]

The Internet Protocol Security Architecture (IPSEC) supports authentication, integrity and confidentiality at the datagram level. Authentication and integrity are provided by appending an authentication header option to the datagram. The authentication header makes use of public-key cryptography methods and openly available algorithms. Confidentiality is provided by the IP encapsulating security payload (ESP). ESP encrypts the datagram payload and header and attaches another cleartext header to the encrypted datagram. ESP can be used to set up private virtual networks within the Internet. Conceptually, ESP performs the same function as the Motorola NES. The strengths of NES are that it works, and that it is certified by the National Security Agency (NSA) to carry classified information. It remains to be seen whether implementations of ESP will be less expensive than NES, will be certified by NSA, and will work better than NES in a multicast environment.

6. Internet Protocol Security Option (IPSO)

The IP Security Option (IPSO) is a set of security features for IP that were proposed in 1991 by the Department of Defense. IPSO consists of labeling datagrams with their level of sensitivity in much the same way that classified documents are labeled

and controlled. IPSO did not include encryption, just flags that routers and hosts could use to facilitate special handling. IPSO is not an Internet Standard, and is not included in all IP implementations. [Atkinson,95]

7. Network Management Security

One element of IP security that has been somewhat neglected is protection of the network devices themselves. The Simple Network Management Protocol version 2 (SNMPv2) was designed to strengthen authentication measures for management of network devices, such as routers [Comer,95]. Many of the original proposed security aspects of SNMPv2 [Galvin,93] were made optional or removed from the Internet Standards track SNMPv2 specification in March 1996 [Postel,96]. A new experimental security protocol for SNMPv2 has been proposed [Waters,96]. Past controversies indicate that successful incorporation of strong security features will not be quickly forthcoming.

8. Other Security Considerations

Because of the inherent insecurity of the Internet infrastructure, many applications have developed their own security features. Privacy Enhanced Mail (PEM) employs sound public-key cryptographic methods to provide security for electronic mail [Bruno,96]. Work is also continuing on a secure hypertext transfer protocol (S-HTTP) for use in Web applications [Rescoria,96]. The IETF is developing a secure protocol for the Domain Name System (DNS) as well [Eastlake,96]. Massive pressure to implement secure commercial electronic transactions on the Internet has produced a variety of simultaneous efforts in this area.

End-to-end security features will play a major role in the Defense Messaging System (DMS). DMS will provide user level authentication and access control, electronic mail authenticity, integrity, confidentiality and non-repudiation, as well as X.500 directory database security controls [Henderson,96]. Thus some security considerations can be handled by applications, independent of the network infrastructure.

At the physical communications layer, key-generated (KG) link encryption devices will continue to be employed throughout the tactical internet to protect against data compromise and traffic analysis [MARCORSYSCOM,95a].

H. SUMMARY

The Internet Protocol is the *de facto* open systems internetworking standard that offers almost universal interoperability. It is independent of the complexities and vagaries that plague various proprietary and hardware-based network protocols. IP's simplicity and robustness have made it enormously popular, not only in the global Internet but also in many large private "intranets." Since IP's development in the 1970s, however, technology has advanced immensely and IPv4 is beginning to show signs of age. The explosive increase in the number of hosts connected to the global Internet coupled with the revolution taking place in mobile computing is beginning to strain the limits of IP's address structure. The demands of real-time, multicast multimedia applications push the bounds of IP's delivery service. The emergence of information warfare as a national priority is further exposing IP's security vulnerabilities. Through it all, however, IP continues to be the networking protocol of choice throughout the world. The IETF and the Internet research community are dedicated to solving the technical problems of the TCP/IP protocol suite. These are good reasons to believe that IPv4 is a sound protocol for the Tactical Data Network. Indeed no suitable alternative exists. Nevertheless IPv4's limitations must be recognized. It is unwise to expect that IPv4 will meet military internetworking needs beyond the current decade.

VI. INTERNET PROTOCOL (IP) VERSION 6

A. INTRODUCTION

The Next Generation Internet Protocol (IPng), now formally called IP version 6 (IPv6), is an evolutionary enhancement of IPv4. IPv6 is designed to redress IPv4's shortfalls, retain IPv4's strong points, and accommodate the expected future growth and diversity of the global Internet. The Internet Engineering Task Force (IETF) has defined the formal structure of IPv6 and this new protocol is on track to become an Internet Standard. IPv6 will eventually replace IPv4 throughout the global Internet and in most private TCP/IP networks around the world. However, the Internet community does not intend for this transition to take place precipitously. Rather, it is expected that IPv6 and IPv4 will coexist for years with transition rates driven by user requirements.

The treatment of IPv6 in this chapter parallels the discussion of IPv4 presented in Chapter V. Following a review of the origin of IPv6 and the progress of its development, the discussion focuses on the same five salient aspects: *addressing, multicast support, mobility support, quality of service (QoS) support,* and *security*. The technical mechanisms that have been defined to facilitate smooth transition from IPv4 to IPv6 are also reviewed. Discussion of the implications of IPv6 on the Tactical Data Network (TDN) architecture completes this chapter.

B. NEED FOR A NEXT GENERATION INTERNET PROTOCOL

The communications field is constantly changing. New technologies are introduced so frequently that older ones must either adapt or become obsolete. Since the original version of IP was developed, computing power has increased by orders of magnitude and the number of machines connected to the global Internet has grown from a few dozen to more than 4 million [Comer,95]. The fact that IPv4 accommodated these changes and continued to grow in popularity is a testament to the soundness of its original design.

However, IPv4 was not originally designed to support a network of universal scale or the interactive multimedia applications being envisioned for the future. IPv4 needs to be upgraded if the Internet Protocol suite is to survive and thrive in the 21st century.

The astonishing growth of the global Internet provided the initial impetus to develop a Next Generation Internet Protocol (IPng) [Hinden,95a]. In 1991 several members of the Internet Engineering Task Force (IETF) concluded that the exponential growth of the Internet threatened to exhaust the IPv4 address space by the end of 1994. Further, the growth in the number of separate networks connecting to the global Internet was causing the Internet's routing tables to fill up, thereby straining the technical capacity of state-of-the-art routing hardware [Bradner, 96a].

The IETF responded to this perceived impending crisis by recommending the adoption of Classless Inter-Domain Routing (CIDR) throughout the Internet in order to delay the exhaustion of addresses [Bradner,96a]. (As discussed in chapter V, CIDR is designed to better utilize the IP address space by allowing flexibility in designing addressing and routing hierarchy.) Initial implementation of CIDR did slow the growth of Internet routing tables temporarily. It is now projected that with widespread implementation of CIDR in the Internet, IPv4 addresses might last until 2020 [Tallerico,95].

Many in the IETF acknowledged that CIDR was as a short-term solution that was merely delaying the inevitable exhaustion of IP addresses. In addition to the growth issue, the nature of the Internet's use was also changing. New technology trends like nomadic computing, interactive multimedia and electronic commerce are emerging. Users want access to all network services via a single network connection, ostensibly the Internet. Convinced that a long-term solution to these challenges required changes to the Internet Protocol itself, in 1992 the IETF solicited proposals from the Internet community for a next generation Internet Protocol to replace IPv4. [Bradner,96a]

C. DEVELOPMENT OF IP VERSION 6

1. Key Players in the Process

The development of the next generation Internet Protocol combines Internet architecture strategy, technical protocol design, and actual protocol software implementation. This subsection identifies the key organizations and participants involved in this development process.

a. The Internet Society (ISOC)

The Internet Society is an international organization concerned with the growth and evolution of the global Internet, as well as with the social, political and technical issues that arise from the use of the Internet. ISOC is composed of both organizational and individual members. The ISOC Board of Trustees oversees the Internet Standards process and ratifies standardization procedures. [Hovey,96]

b. The Internet Architecture Board (IAB)

The Internet Architecture Board is chartered by the ISOC to provide oversight of the architecture and the protocols of the global Internet. The IAB advises the ISOC and the IETF regarding technical, architectural, policy and procedural matters pertaining the technologies of the Internet. The IAB performs strategic planning and identifies long range problems and opportunities. [Hovey,96]

c. Internet Engineering Task Force (IETF)

The Internet Engineering Task Force is a loosely organized group of technical professionals who make contributions to the technological evolution of the global Internet. It is the principal body involved in development of specifications for protocols used on the Internet. The IETF is composed of numerous (currently 76) *Working Groups* that are grouped into nine *Technical Areas*. IETF Working Groups are intentionally short-term entities focusing on solving specific problems or developing specific

protocols. Participation in the Working Groups is open to anyone who has enough time and interest. Much of each group's collaboration is done via e-mail. Participants contribute as individuals, not as representatives of organizations. [Hovey,96]

The open and egalitarian nature of the IETF's procedures contrasts with those of other standards developing bodies. For example, the International Telecommunications Union (ITU) and the International Organization for Standards (ISO) both tend to be dominated by the interests of telecommunications corporations and public communications utilities [Baker,94]. The open nature of the Internet standards process has been a major factor in the widespread acceptance and use of TCP/IP protocols.

d. IPng Working Group

A special IETF working group was created to direct the development of IPv6. The IPng Working Group (IPngWG) has cognizance over the development of the initial specifications for IPv6. Responsibility for the various aspects of IPv6 will eventually shift to the cognizant functional Technical Areas, and the IPngWG will be (successfully) dissolved. As of this writing, the IPng Working Group is still refining specifications for IPv6. Information about the current progress of IPv6 is available at

http://playground.sun.com/pub/ipng/html/ipng-main.html
and *http://www.ietf.cnri.reston.va.us/html.charters/ipngwg-charter.html*

e. Internet Engineering Steering Group (IESG)

The Internet Engineering Steering Group manages the technical activities of the IETF. Composed of the IETF Chairperson and the Directors of the IETF Technical Areas, the IESG administers the Internet standards process and is the deciding authority as to whether a protocol specification is advanced along the "standards track." [Hovey,96]

f. Research Laboratories and Commercial Protocol Software Vendors

Research laboratories and commercial vendors play a vital role in the Internet standards process. Although the IETF defines protocol specifications, it is up to software programmers at research laboratories and commercial vendors to produce working

protocol implementations. Working implementations are key because a protocol must be successfully and independently implemented twice in an operational environment before it can become an Internet *Draft Standard.* Software implementations usually follow shortly after Internet protocol specifications are defined because many of the working groups' participants are associated with commercial protocol software/hardware vendors and research labs.

2. Selecting an IPng Proposal

In 1993 the IESG chartered the IPng Working Group (IPngWG) to develop a recommendation for the Next Generation Internet Protocol. The IPngWG evaluated three candidate protocol proposals and selected the Simple Internet Protocol Plus (SIPP) as the best of the three. SIPP was the proposal that differed least from IPv4, had the most details defined and (most importantly) had the best-thought-out transition plan. [Bradner,96a]

The finalized IPng recommendation presented to the IETF by IPng Working Group in 1994 was actually a synthesis of the three candidate proposals, combining the best aspects of each one. The IPngWG recommendation was approved by the IETF in November 1994 as the basis for IPv6. [Bradner,96a]

3. Moving Forward: The Internet Standards Process

To ensure that IPv6 will be widely accepted and implemented throughout the Internet, the IETF plans to make IPv6 an *Internet Standard.* An Internet Standard is a protocol specification that is well understood, technically sound, and has multiple interoperable implementations that have worked successfully in operational networking environments [Bradner,96b]. IPv4 (also referred to as STD-5) is an example of an Internet Standard. This section briefly explains the Internet community's standards process to help the reader to understand IPv6's current stage of maturity.

The Internet standards process focuses on practicality, simplicity and timeliness. Before becoming an Internet Standard a protocol must be proven to work. Protocol

documentation must be clear, concise and easy to understand. Finally a protocol must achieve success and acceptance within two years or it will normally be removed from the "standards track." [Bradner,96b]

The IETF has defined a "standards track" to provide order to the standards development and approval process. A protocol that is expected to become a standard must evolve through the three stages of maturity in the track: *Proposed Standard, Draft Standard* and *Internet Standard.* [Bradner,96b]

a. Proposed Standard

A protocol advanced to the status of *Proposed Standard* is officially on the standards track. At the time of this writing most of the core IPv6 specifications have become Proposed Standards [Postel,96]. A proposed standard has the following characteristics:

- well-known design choices have been resolved
- is well understood
- has received significant review by the Internet community
- appears to enjoy interest and support
- has not yet been implemented operationally
- may be changed or even retracted if experience is not positive

Protocol specifications are declared proposed standards only by decision of the IESG. Before an official IESG decision is made, the cognizant IETF working group usually releases its working draft of the protocol specification to the Internet community. These *Internet Drafts* invite informal comments regarding refinement of the specification. Once the IESG approves the specification as a *Proposed Standard,* the specification is published as a *Request for Comments (RFC).* Each RFC is given a unique number, and the protocol specification is always identified with that RFC number

throughout its lifetime. A protocol must remain in *Proposed Standard* status for a minimum of six months before it can be considered for advancement to *Draft Standard.* [Bradner,96b]

b. Draft Standard

A protocol specification advanced to *Draft Standard* is almost certain to become an *Internet Standard.* Draft standards usually have at least two interoperable real-world implementations with substantial operational experience. Specifications must remain in *Draft Standard* status for at least four months before being considered for advancement to *Internet Standard.* Vendors can safely begin commercial implementations of a protocol in this stage of maturity because it is unlikely to change before becoming a standard [Bradner,96b]. At the time of this writing none of the IPv6 specifications have yet become Draft Standards [Postel,96].

c. Internet Standard

Internet Standards are highly mature protocol specifications with successful and stable operational implementations. A standard can be classified as *required, recommended* or *elective*. A required standard must be implemented by any system claiming to be TCP/IP compliant. As an example, IPv4 is a required standard. TCP, on the other hand, is a recommended standard. If another transport layer protocol better satisfies a vendor's needs, the vendor does not have to implement TCP in his "TCP/IP stack." However the IETF strongly encourages vendors to include recommended standards in all implementations. Finally, implementation of elective standards by vendors is optional. [Bradner,96b]

The current status of all Internet protocol specifications is contained in *Internet Official Protocol Standards* (STD-1) which is updated and published quarterly as an RFC [Postel,96]. Every Internet Standard is documented in an RFC, but not every RFC is an Internet Standard. [Bradner,96b]

4. Current State of Progress in IPv6 Development

a. IETF Protocol Work

Much of the technical protocol specification work for IPv6 has already been completed. The details of the IPv6 packet structure, addressing architecture and security architecture have been approved as Proposed Standards [Postel,96]. Some of the peripheral protocols that will interact with IPv6 are not yet fully specified, and work continues on several IPv6 packet extension headers. The specification for IPv6 mobility support [Perkins,96a] is still in draft stage at the time of this writing. Likewise quality of service (QoS) functionality has not been completely defined. IPv6 support for mobility and QoS are subjects of continued research and are discussed later in this chapter.

b. Host Implementations

The basic structure of IPv6 has stabilized and vendors and laboratories have begun development of IPv6 software that can be implemented on host computers (end systems). Commercial IPv6 prototype software is being developed by Sun Microsystems Inc. and Hewlett-Packard Inc. among others. Product versions of IPv6 software are expected to be available by the end of 1997 [Medlin,96]. Further, the Institut National de Recherche en Infromatique et en Automatique (INRIA) and the Naval Research Laboratory (NRL) have each developed an experimental IPv6 host implementation based on the Berkeley Software Design (BSD) version of UNIX [Tallerico,95]. Current information regarding host implementations of IPv6 software is tracked by the IPng Working Group of the IETF and is posted on the IPng Web page [Hinden,96] at

http://playground.sun.com/pub/ipng/html/ipng-main.html

c. Router Implementations

Development of IPv6 router implementations has been slower than development of host implementations. The main reason for this problem is that key aspects of IPv6 routing have not been fully defined. Nonetheless, several commercial router vendors are developing preliminary versions of IPv6 routing software anyway. Cisco Systems Inc., Bay Networks Inc. (*Wellfleet* routers) and Ipsilon Networks Inc. all have prototype IPv6 routing implementations, but none of these companies has made source code publicly available [Reitzel,96]. Progress on router implementations is also maintained on the IPng Web page [Hinden,96].

d. IPv6 Implementation Testing

Preliminary third-party testing of the INRIA prototype IPv6 host implementation was conducted by Mitre Corporation in 1995. The test results are promising. Mitre successfully used IPv6 to establish TELNET and FTP sessions between two hosts on the same physical network. Further, Mitre was able to "tunnel" IPv6 packets between two IPv6 hosts using an IPv4-only network backbone. This tunneling capability is a key IPv6 transition mechanism, and is described in more detail later in this chapter. [Tallerico,95]

Thus far the only public testing of IPv6 router implementations was conducted at the University of New Hampshire (UNH) Interoperability Laboratory in February 1996. Most of the U.S. vendors and laboratories who had any type of prototype IPv6 software (host or router) demonstrated it at the UNH event. Initial reports from participants [Grehan,96] suggested that most implementations were highly successful, but no documentation of the test results has been released. The testing plan for the UNH event is available at

http://www.iol.unh.edu/general/IOL-News_Items/IP-1-22-96.html

5. Future Developments to Watch

Progress in the development of routing implementations will be a barometer for gauging the maturity of IPv6. In order for a network to fully benefit from IPv6's increased address space, reduced packet processing overhead, quality of service controls, native multicast capability and embedded security, IPv6 software must be implemented in the network's routers. Large-scale transition from IPv4 to IPv6 will not be feasible until stable IPv6 routing implementations are available. The IPng Working Group has recognized this fact and is endeavoring to establish an IPv6 "backbone" within the Internet to study and test IPv6 implementations similar to the way MBone is employed now to study multicast [Reitzel,96]. Thus far the "6-Bone" plan has been stymied because no IPv6 routing software code is publicly available [Reitzel,96]. It is wise for the Marine Corps, DISA and the other military services to track this IETF project closely because it is likely to unearth problems that tactical and strategic networks might encounter when making the transition from IPv4 to IPv6.

D. OVERVIEW OF THE IPV6 SPECIFICATIONS

IPv6 does not represent a *revolutionary* replacement of the Internet Protocol. Rather, it is an *evolutionary* step forward from IPv4. IPv6 retains the fundamental connectionless packet delivery service of IPv4 but also adds new functionality to improve scalability and to support a broader range of applications. The major improvements of IPv6 over IPv4 include [Tallerico,95]:

- Expansion of the address space and a more versatile address hierarchy.
- A new type of addressing called *anycast* that is conceptually a cross between unicast and multicast.
- Allowable use of non-globally unique *(link-local* and *site-local*) addresses on networks that are connected to the global Internet.
- IP address autoconfiguration that enables "plug and play" connection to the network.

- A simplified IP packet header to reduce the per-packet computational load on network routers.
- Provision for future addition of protocol features through use of extension headers.
- Native multicast capability (IP Multicast) and an improved mechanism for controlling the scope of multicast sessions.
- A new *flow label* field in the IPv6 packet header that provides a mechanism for controlling quality of service (QoS).
- Elimination of IPv4 requirements that were determined to be redundant during IPv4 operational experience.
- Native support for security at the IP (internet) layer.

The IPng Working Group has also developed a number of protocol mechanisms that allow IPv4 and IPv6 to coexist within a network in order to facilitate a smooth transition to IPv6. Each of the capabilities listed above and the corresponding transition mechanisms are discussed in further detail in the following sections.

E. IPV6 ADDRESSING

1. Overview of IPv6 Addressing

The original impetus for the IPv6 development was the need for more IP address space. Therefore many of the differences between IPv4 and IPv6 relate to addressing. This section discusses the IP address format and hierarchical structure, the new address type called anycast, IPv6 address autoconfiguration, and IPv6 routing considerations.

2. IPv6 Address Format

a. Address Notation in IPv6

IPv6's most visible and well known feature is its 128-bit address. The current 32-bit IPv4 address is composed of four 8-bit octets, and is usually written in a *dotted decimal* form (e.g. *131.120.50.202*). The 128-bit IPv6 address is composed of *eight* 16-bit *double octets*. This makes the IPv6 address awkward to represent in decimal form.

Instead, IPv6 addresses are expressed as hexadecimal (base 16) numbers (one hex number for each double octet) separated by colons. An example IPv6 address in this *colon-hex* notation is *153F:102A:1224:67A4:903F:65EA:7898:78A4*. In practice it is expected that many IPv6 addresses will contain several zero-valued double-octets. For brevity a string of zero valued double-octets is represented by a double colon. For example, the address *10A4:0:0:0:0:3A23:1178:2345* can be written more compactly as *10A4::3A23:1178:2345*. IPv4 addresses in dotted decimal notation can be easily converted to colon-hex notation by adding the double colon to the left of the first octet as in this example: *::131.120.50.202*. The latter notation maps IPv4 addresses into the IPv6 address space, and is one of the transition mechanisms discussed in Section J of this chapter [Carl-Mitchell,95].

The 128-bit IPv6 address length was a compromise between the IETF members who wanted to accommodate immense growth of Internet address requirements and those IETF members who wanted to constrain IP overhead in order to accommodate mobile Internet users (who presumably access the network over low bandwidth communications links using less powerful computers). The IPv6 address space is indeed immense. Theoretically, more that 100 million unique IPv6 addresses could be assigned to every person alive in the world today and there would still be millions of addresses left over. In fact only 15 percent of the IPv6 address space has been allocated for use. The remaining 85 percent is reserved for future requirements [Hinden,95b].

b. Addressing Hierarchy in IPv6

The increased length of IPv6 addresses permits greater flexibility in defining the addressing hierarchy. The original IPv4 address space had only one level of hierarchy and three classes (network sizes). Classless Inter-Domain Routing (CIDR) expanded the IPv4 address hierarchy somewhat by allowing a 32-bit IPv4 address to be partitioned arbitrarily between *networkID* and *hostID*. The method of indicating address hierarchy in IPv6 is essentially the same as the method used for CIDR. However, IPv4's 32-bit

address length severely limits the levels of hierarchy that CIDR can define. The fact that a substantial portion of the total IPv4 address space has already been allocated using the less efficient three-class structure further restricts the effectiveness of CIDR.

The IPv6 address allocation architecture [Rekhter,95] seeks to support decentralized administration of address assignment and to reduce the amount of computation, memory and bandwidth consumed by routing. Both of these goals are attainable through *hierarchical* addressing and routing. By partitioning the IPv6 address into several hierarchical tiers, large blocks of addresses can be allocated to international or regional address assignment authorities. Those address blocks can be further partitioned and the control of assignment within blocks can be passed down the hierarchy. Below each level of the hierarchy every host and router shares a common address prefix. This greatly reduces the amount of routing information that must be exchanged among routers (particularly routers on the backbone). Currently all IPv4 address assignments are made by a central authority (InterNIC) and there need not be any correlation between two network number assignments, regardless of physical or logical proximity. For example, the Marine Corps can be assigned two unrelated IP network address blocks for two networks that are on the same Marine Corps base. [Rekhter,95]

A hierarchical IPv6 address allocation plan called the *Provider-Based Unicast Address Format* is currently in draft stage [Rekhter,96b]. This plan defines a three-tiered hierarchy consisting of registries, providers, and subscribers. Addresses are partitioned as depicted in Figure 6.1 below.

3	5 bits	n bits	56-n bits	64 bits
010	Registry ID	ProviderID	Subscriber ID	Intra-Subscriber

Figure 6.1 Proposed IPv6 Unicast Address Format. After [Rekhter,96b].

The leftmost three bits indicate that this a unicast address. The *Registry ID* identifies the IPv6 address assignment authority that assigned the address. Registries are expected to encompass broad geographic areas, and currently only four IPv6 address registries have been identified. The Internet Assigned Number Authority (IANA) will serve as the principal global IPv6 address registry and will assign large blocks of addresses to three other regional registries. The registries can then allocate blocks of addresses to providers (operators of transit IP networks). The *Provider ID* identifies the Internet provider from which the address is obtained. The *Subscriber ID* identifies the major organization (e.g. corporation, campus, military base) to which the address belongs, and the *Intrasubscriber* portion can be allocated as the subscriber sees fit. There is no prescribed length for the *Provider ID* or the *Subscriber ID* but both together must total 56 bits. Each of the fields in this proposed address format can be further subdivided using a procedure much like the subnetting described in Chapter V. [Rekhter,96b]

It is not clear where the military services will fit into this address hierarchy. A separate military registry will probably not be necessary. It is more likely that the Defense Information Systems Agency (DISA) will be considered the Internet *provider*, since it provides NIPRNET and SIPRNET connectivity for the military, and each service will be issued *subscriber* blocks of addresses.

3. IPv6 Address Types

In precise terms, Internet Protocol (IP) addresses refer to specific network *interfaces* rather than specific network *nodes* [Comer,95]. The distinction is subtle but important. The term *node* implies a single machine that is physically connected to the internet. A network *interface* is a more specific identity than either *host* or *node*, because a host or node can have multiple physical and logical network interfaces. For example, a router (node) has at least two ports, each of which physically connects to a different network. Therefore a router has at least two network interfaces. A network interface can also be logical. For example, a domain name server and Web server that reside on the

same host computer may have different *logical* network names and interfaces, even though their host may have only one *physical* network interface [Bradner,96a]. The distinction between interfaces and nodes is helpful in understanding IPv6 address types.

The IPv6 addressing architecture [Hinden,95b] defines three types of addresses: *unicast, multicast*, and *anycast*. Of significant note is that IPv4-style broadcasting is no longer used because it wastes bandwidth and processing time. A unicast address identifies a single network interface such that a packet sent to a unicast address is delivered to only that one interface. A multicast address identifies a set of interfaces such that a packet sent to a multicast address is delivered to *every* interface in the set. Conceptually, unicast and multicast are identical in both IPv6 and IPv4. The *anycast* address (also referred to as a *cluster* address) is a new concept introduced by IPv6. Anycasting is discussed in the next section. [Hinden,95b]

4. Anycasting

Functionally, anycast is a cross between unicast and multicast. An anycast address identifies a set of interfaces (anycast group) such that a packet sent to an anycast address is *delivered to only one of the interfaces in the set*. The interface to which the packet is delivered is the one determined by the routing algorithm to be the "closest." There is no way to distinguish an anycast address from a unicast address syntactically, i.e. by inspection. Anycast and unicast addresses are both assigned from the unicast address space. Nodes must be specifically configured to recognize a particular IPv6 address as belonging to an anycast group. The IETF has not specified a method for managing anycasting. One proposed method [Partridge,93] employs the same techniques and protocols that are used in managing IP Multicast groups. [Hinden,95b]

Anycasting is immature and its application is not well understood. The Internet community envisions using anycasting to support *policy-based routing*. Policy-based routing is the exerting of control over the geographical and topological flow of data packets through the internet (much like source routing in IPv4). The Internet community

believes that organizations and individuals who are paying for Internet services from specific providers need a means of assuring that *their* chosen provider transports *their* data traffic. To provide such assurance each Internet provider might be assigned his own anycast address that identifies all of that provider's routers. Inserting the provider's anycast address in an IPv6 packet header is intended to ensure that the packet will transit the provider's network. [Bradner,96a]

It is less clear how the military might apply anycasting to enforce policy-based routing. Secure routing is one possible application. The military's widespread use of link encryption makes its data networks more secure than commercial and public networks. Furthermore, the military has little control over the bandwidth/switching capacity and allocation schemes of outside networks. Therefore it makes sense to transport military data traffic over military networks as much as possible. The suggestion has also been made to use policy-based routing to segment different data types onto specific subnetworks within the tactical internet [Adamson,96]. It is not clear whether using anycast addresses can support this segmentation.

There are many other potential uses for anycasting besides policy-based routing. Morales [96] proposes employing anycast addresses to deliver Defense Messaging System (DMS) data traffic to Navy ships at sea. Anycasting can also be applied in the tactical internet to make it easier for end users to locate well-known network services. (This process is often called *resource location.*) In order to ensure a high degree of availability the tactical internet must have distributed and mirrored databases and servers, i.e. multiple sites containing identical information. Users who access geoposition databases, Web servers and DNS name servers do not really care which specific computer supplies the information as long as the information is accurate, timely and complete. Therefore, a single anycast address might be assigned to a group of mirrored databases or Web servers to make them easier to find. When a user sends a packet to that anycast address, the server that is nearest the user will respond. Similarly a single anycast address might also be consistently assigned to all of the Domain Name System (DNS)

servers within the Marine Corps Tactical Data Network. This eliminates the need to configure each host with the address of its local name server because anycasting reaches the nearest server by default. In each of the examples given above the actual location of the server is initially transparent to the user. This is an advantage in a network as mobile and rapidly changing as the Marine Corps tactical internet.

Some protocol interface details will have to be worked out in practice to make IPv6 anycast addresses usable by current higher layers. The use of anycasting (a connectionless process) for resource location might confuse a connection-oriented protocol like TCP. A TCP connection is only established between two end points. However anycasting cannot guarantee that the same end point (server or database in this example) will receive *all* of the anycast packets because the network's routers have no way to keep track of where previous anycast packets were delivered. Depending on network topology changes and the routing algorithms in use, the first packet of a TCP connection might go to one server and the second packet to a different server. This is a situation that TCP cannot handle. One solution to this problem is to use anycasting to make the initial contact with the server and then have the server reply with its own unicast address (i.e. locate the resource). A unicast TCP connection might then be established using unicast addresses. [Partridge,93]

It is useful to compare anycasting and multicasting for locating resources. The most important advantages of using anycasting for this purpose in the tactical internet are bandwidth conservation and routing simplicity. Resource location with multicasting often involves sending multiple datagrams over multiple paths. Using anycast, only one packet is sent (assuming no packet loss) over one path to the nearest server. Further, multicast routing is more complex than the unicast routing needed for anycast. [Partridge,93]

Anycasting also raises several security concerns. Anycasting promotes network security in that the actual IP addresses of well-known network services do not need to be published to end users. Only after authenticating a client will the server reply with its

own IP address (in the case of TCP connections). Thus an anycast IP address can shield a server or database from attack to some degree. However anycasting also introduces security vulnerabilities. A malicious host or software program might "volunteer" to be a server in an anycast address group and feed false information to clients [Partridge,93]. Malicious software might also conduct a denial-of-service attack by joining the anycast group and simply accepting (but not replying) all data traffic sent to the anycast address. Thus far the IPng Working Group has tried to reduce the security risks of anycasting by specifying in the IPv6 addressing architecture "an anycast address MUST NOT be assigned to an IPv6 host, that is, it may be assigned to an IPv6 router only" [Hinden,95b]. This rule severely restricts the applications of anycast in the tactical internet. All in all, anycast addressing has promising potential but a more suitable security solution for anycast vulnerabilities must be found.

5. Address Autoconfiguration in IPv6

Autoconfiguration enables "plug-and-play" connection to the network. Address autoconfiguration is a feature that allows a host to legitimately acquire one or more IP addresses for itself and to associate those addresses with the host's network interface. A host's IP addresses need to be configured each time a network interface is initialized, which normally occurs when the computer boots up [Bradner,96a]. A interface must be reconfigured whenever its IP address changes, such as when the host is moved to a different subnetwork. As described in Chapter V, configuration/reconfiguration is typically done manually by systems administrators. With the advent of multiple addresses per host and widespread mobility of end-user computing devices, manual address configuration will no longer be feasible. Further, it is likely that portions of the Internet will have to be renumbered after the introduction of IPv6. This process must be made as "painless" as possible to facilitate the IPv4 to IPv6 transition. Therefore, another goal of the IPv6 specification is to allow plug-and-play connection (and reconnection) to the Internet. Although autoconfiguration has been employed for a number of years in

local-area networking (data link layer) technologies such as Novell NetWare and AppleTalk, there has been much less experience with IP layer autoconfiguration.[Bradner,96a]

IPv6 has two methods of autoconfiguration: *stateful* and *stateless*. Stateful autoconfiguration will be accomplished by an updated version of the Dynamic Host Configuration Protocol (DHCP) that was described in Chapter V. The stateful method requires the DHCP server to have prior knowledge of the state (e.g. how many hosts) of the link on which it is assigning addresses. The stateless method requires no manual configuration of hosts and does not depend upon the presence of servers. Hosts are permitted to form their own addresses by combining a unique "network interface token" (probably the unique 48-bit Ethernet hardware address) with the subnet prefix that is periodically advertised by the local router. The stateless method of autoconfiguration is meant to be used in networks where the specific address used by an interface is not really important as long as the address is unique and routable. Such a system may not work locally if the network managers want to predefine addresses down to the host level. [Thomson,95]

Another feature of IPv6 that facilitates plug-and-play operation is the addition of *site-local* and *link-local* addressing. Every host will have a link-local address that can be used for IP communications on the physical link to which the host is attached. Routers will not forward packets containing link-local addresses, so link-local addresses are limited to use local LAN segments. Site-local addresses use a reserved portion of the global IPv6 address space, but do not need to be assigned by a global addressing authority. Site-local addresses are intended to be used on networks that are not currently connected to the global Internet but may establish an Internet connection in the future. If the network eventually is connected to the Internet, its site-local addresses can be retained and used with the addition of a globally-unique *subscriber ID* address prefix. Link-local and site-local addresses greatly expand the number of addresses that can be used by an organization. However, it does not appear wise to use link-local and site-local addresses

in the tactical internet. The IPv6 address space is so huge that sufficient globally unique addresses can be obtained to accommodate both current requirements and future growth of the Tactical Data Network (TDN). [Hinden,95b]

6. IPv6 Routing Considerations

Routing and addressing are inextricably linked in TCP/IP internetworking. One of the key design goals of IPv6 was to simplify routing by introducing global addressing hierarchy and streamlining the IPv6 packet header [Bradner,96a]. Although the IPv6 address is four times larger than the IPv4 address, the IPv6 header is only twice as large as the IPv4 header [Deering,95]. Furthermore, routing option information was moved out of the basic IPv6 packet header and into new packet extension headers. The significance of this design is that (unlike IPv4) intermediate routers using IPv6 need not inspect the optional extension information, so routing is simpler [Carl-Mitchell,95]. It remains to be seen in practice whether the per-packet costs of routing IPv6 will be less than those of IPv4.

Another routing simplification feature of IPv6 is the elimination of packet fragmentation by intermediate nodes. If an IPv4 datagram is too large for a data link layer protocol to handle, any IPv4 router can break the datagram into smaller pieces (fragment it) for transmission over that link. The datagram is reassembled (de-fragmented) by the next IPv4 router in the path. Because fragmentation is computationally expensive, only the source and destination nodes are allowed to fragment an IPv6 packet. This requires the IPv6 end nodes to discover the largest packet size (called MTU) that can traverse the entire path (route) without having to be fragmented. Indeed, a protocol for MTU discovery in IPv6 is now in draft stage [McCann,96]. However, end nodes can also choose to forego MTU discovery by restricting the size of packets to 576 bytes (the minimum packet size that IPv6 networks must transport) [Deering,95].

Routers using IPv4-only routing software will not be able to route native IPv6 packets. Nor will IPv6-only routing software handle native IPv4 packets. The packet sizes and structures of the two protocols are different and the address hierarchies are dissimilar. (Section J of this chapter discusses protocol mechanisms that allow IPv4-IPv6 interoperability.) However, conceptually IPv6 routing will be much like IPv4 routing [Bradner,96a]. The standard IPv4 routing protocols now being used in most TCP/IP networks, namely Open Shortest Path First version 2 (OSPFv2) and Border Gateway Protocol 4 (BGP-4), will be upgraded to handle IPv6's longer addresses and new packet format [Tallerico,95]. It is likely that deployed IPv6 routing software will still retain backwards compatibility with IPv4 packets.

7. IPv6 Addressing Summary

The Tactical Data Network (TDN) architecture must include provisions for transitioning to IPv6 addressing. The hierarchical structure of IPv6 addresses will significantly impact the TDN tactical IP address plan and the routing of datagrams through the tactical internet. Autoconfiguration is needed to simplify network administration, allow plug-and-play TDN connectivity and facilitate mobility. Finally, anycasting will provide a powerful tool for making the network infrastructure more transparent to end systems.

F. IPV6 MULTICAST SUPPORT

Multicast support in IPv6 is not substantially different from IPv4 (IP Multicast). The most significant change is that all IPv6 implementations must have native multicast capability. This will eliminate the need to tunnel multicast packets across unicast-only routers in the way that MBone does today. This universal multicast capability must be exploited by both the tactical internet architects and the developers of tactical applications software. Multicast capability inherent in lower-level networking technology is only part of the solution. Higher-layer applications must also be configured to take advantage of the multicast support provided by the lower protocol layers.

IPv6 does not address the reliable multicast requirement specifically, since reliable multicast is a transport layer function and not an internet layer function. IPv6 must fulfill the requirements of a bearer service and support a broad range of higher-layer applications. Thus quality of service features such as reliability cannot be "hard coded" into the baseline Internet Protocol.

The Marine Corps C4I development community needs to track multicast research efforts such as the MBone [Kumar,96b], and also follow the multicast development efforts of commercial firms such as Starburst Communications [Starburst,96]. Transport layer protocols must be devised that support reliable multicast in ways that are implementable and scaleable [Knight,96]. Finally, multicast capability must be made a requirement for new and re-engineered software applications.

G. IPV6 MOBILITY SUPPORT

Support for mobile hosts, networks and subnetworks is a primary design requirement for IPv6 [Bradner,96a]. The protocol specification for mobility support in IPv6 is in draft form and is similar to the Mobile IP protocol described in Chapter V. IPv6 improves upon Mobile IP by reducing the importance of the *home agent*, allowing direct communication between mobile nodes and other nodes in the internet. Using IPv6 a mobile node can make its current IP address known to the other nodes (mobile or stationary) with which the mobile node is communicating. These other "correspondent" nodes can then communicate directly with the mobile node without going through the mobile node's *home agent*. For security reasons the mobile node need not reveal its current IP address to any node except its own *home agent*. Therefore, IPv6 can employ either direct or indirect (tunneling) routing to support mobile nodes. Another significant change in the IPv6 mobility plan is that it requires all routers in the network to be capable of acting as home agents. Thus mobility support is assured in all portions of the internet that are employing IPv6. [Perkins,96a]

IPv6 does not address how a mobile node is to maintain TCP connections while changing IP addresses. (TCP uses the IP addresses and port numbers of the end points to identify a connection.) This points to the need for an integrated mobility solution that encompasses the transport and internet protocol layers. However, the draft IPv6 mobility plan does mention a potential security problem that might result from mobile nodes trying to access networks which are protected by firewalls [Perkins,96a]. Firewalls that filter packets on the basis of the packet's source address might deny access to a mobile node that has moved to an "untrusted" network. The IPv6 plan does not propose a solution to this problem but stresses the need for one [Perkins,96a]. This further illuminates the inadequacy of address-based and name-based authentication methods (as discussed in Chapter V) and reinforces the requirement for integral, robust packet security features in IPv6.

Seamless access to network services is a required objective capability of the tactical internet [MCCDC,95a]. Although neither Mobile IP nor IPv6 offer complete solutions to mobile computing, the Internet community is continuing active research in this area. Mobile IP is too immature at this point for the Marine Corps to make a final decision as to whether to implement it in TDN. The preferred solution is an open system standard that will be widely implemented and available in commercial software. Nonetheless, other internet mobility solutions such as the Army's proprietary Tactical Name Server (TNS) must be evaluated for potential incorporation into TDN in case the open systems protocol does not develop fast enough. Market forces and similar design requirements make it likely that Mobile IP will become robust enough to meet Marine Corps needs in a timely manner.

H. IPV6 QUALITY OF SERVICE (QOS) SUPPORT

Besides the need to increase address space, quality of service (QoS) support was the most important feature that needed to be designed into IPv6 [Bradner,96a]. IPv6 will offer a choice of QoS levels beyond the single "best effort" delivery service offered by

IPv4. With these added QoS capabilities IPv6 will provide a better range of support to real-time data traffic. Although IPv6's QoS features are anxiously anticipated by the Internet community, these features are still in the experimental stage of development [Deering,95].

The primary QoS mechanisms provided by IPv6 are the *flow label* and *priority* fields of the IPv6 data packet header. A flow is a sequence of data packets sent from a particular source (usually a single host) to a destination for which the source (or sender) desires special handling by the network [Deering,95]. A flow is analogous to a virtual circuit or a connection. Figure 6.2 lists some data traffic types that can be classified as flow-oriented, contrasted with non-flow-oriented data traffic which typically consists of only a few packets. A flow is uniquely identified by the combination of the packet's source address and non-zero value in the packet's flow label field. An IPv6 packets that is not part of a flow has a *flow label* value of zero and receives the internet's default best-effort delivery service. [Deering,95]

IPv6 does not specify exactly *how* the flow label is to be used. Of course the type of special handling required or desired for a particular flow must be communicated to the network's routers (QoS negotiation) by some means. The emerging standard for QoS negotiation over IP is the Resource Reservation Protocol (RSVP) [Braden,96]. Hosts and routers use RSVP to deliver QoS requests to all nodes along the path of the data stream, typically resulting in a reservation of bandwidth for that particular data flow.

FLOW-ORIENTED TRAFFIC	SHORT-LIVED TRAFFIC
file transfer protocol (FTP) data	Domain Name System (DNS) query
TELNET session	Simple Mail Transfer Protocol (SMTP) data
Hypertext Transfer Protocol (HTTP) data	Network timing protocol (NTP)
Web image download	Point-of-presence (POP)
Multimedia audio/video	SNMP network management queries
Distribute Interactive Simulation (DIS) streams	

Figure 6.2 Flow-oriented data versus non-flow-oriented data. [Ipsilon,96]

Since RSVP is designed for use over both IPv4 and IPv6, it does not make use of the *flow label* field in the IPv6 packet header [Braden,96]. The details of RSVP are currently being worked out experimentally, while the major router vendors have expressed plans to support RSVP in the near future [Rogers,96].

The *priority field* label specifies the delivery priority of data packets *relative to the other data packets from the same source* [Deering,95]. All packets belonging to a particular flow must have the same priority, so prioritization can also be done by *flow label*. It is expected that the *priority field* will be used to identify interactive and control-oriented data traffic as having higher priority than electronic mail and other non-interactive applications [Bradner,96a]. This prioritization by data type falls short of the tactical internet's requirement for *prioritization among sources* noted in Chapter IV. Therefore a priority mechanism must be employed within TDN in addition to the IPv6 *priority field*. This may require explicit reservations of bandwidth on intermediate routers for the highest priority users or end systems.

As in the cases of multicast, mobility and security, IPv6 is not the complete solution to TDN's quality of service requirements. Ensuring end-to-end QoS requires a cooperative effort between the end-user applications, the transport and internet layer protocols, intermediate routers and the underlying physical network. This is an immensely complex problem involving QoS negotiation methods, appropriate routing metrics, and authentication mechanisms [Borden,95]. Of particular concern to the Marine Corps and the other military services is how IPv6 and Asynchronous Transfer Mode (ATM) might coexist and complement one another. DISA plans to migrate to an ATM-based joint tactical communications architecture in the near term, but has not specified the extent of ATM deployment within the joint network [JIEO,95a]. The likely architecture will be a mixture of IP routers and ATM switches in the internetwork and a few pockets of ATM LANs. Although unicast IPv4-over-ATM has been feasible for several years, it is not at all clear how IPv6 can mesh its QoS capability with that of ATM. For example, there are fundamental differences between RSVP's QoS negotiation

method and ATM signaling. (An extensive treatment of issues regarding integration of IP and ATM quality of service controls can be found in [Borden,95]). Further complicating the issue are both the inherent complexity of ATM, lack of many-to-many multicast in ATM, and the fact that no single and stable ATM standards process has yet emerged.

A proprietary solution to IPv4-ATM integration called *IP Switching* has been developed by Ipsilon Networks [Ipsilon,96]. IP switches dynamically choose between IP routing (in software) and ATM switching (in hardware) depending on the nature of the data traffic. This technology sounds promising but it relies on proprietary protocols which may restrict its availability and multi-source competition. An open systems solution is being pursued collaboratively by the IP-over-ATM and Integrated Services Working Groups of the IETF. Several draft proposals for IPv6 over ATM are being evaluated [Armitrage,96], but it may be several years before any widely acceptable and implementable solution is found. Current information regarding the progress of these efforts can be found at the working groups Web pages [Hinden,96] at

http://www.ietf.cnri.reston.va.us/htmlcharters/ipatm-charter.html and
http://www.ietf.cnri.reston.va.us/htmlcharters/intserv-charter.html

IPv6 will be a quantum leap forward from IPv4 in terms of providing QoS support. Although massive bandwidth can eliminate many QoS bottlenecks [Brutzman,96], such bandwidth is unlikely to be available within the tactical internet. Therefore it is expected that tactical applications will develop more detailed and more demanding requirements for delivery control. Furthermore a requirement will emerge to integrate quality of service guarantees across the disparate networking technologies of the tactical internet. The Internet community and commercial vendors are actively pursuing methods of making varied internetworking technologies like IP and ATM interoperate seamlessly. The prudent course of action over the next one-to-two years is to remain patient and allow these solutions to materialize.

I. IPV6 SECURITY

Security in the Internet is such a critical problem that solutions must be developed and implemented without waiting for IPv6. The IPv4 security architecture outlined in Chapter IV extends to IPv6 as well. Differences are confined to the method of implementation in the packet headers. The *Security Architecture for the Internet Protocol* [Atkinson,95] is on the standards track as a Proposed Standard [Postel,96].

When IPv6 is deployed, network infrastructure security will become even more important than it is now. IPv6 mobility support requires that mobile nodes are authenticated before joining the network, and meanwhile the mobile node's own location must be protected from those in the network who don't have a "need to know." Autoconfiguration mechanisms (DHCP and DNS) might be exploited by network intruders if proper authentication procedures are not enforced at the network level. Unprotected quality of service options in IPv6 might increase the vulnerability of the tactical internet to both intentional and unintentional denial-of-service attacks. Finally as the military becomes more network-centric in its approach to C4I, control and disruption of the network infrastructure devices themselves becomes a more likely avenue of attack for information warfare. The IETF recognizes these issues and has done substantial work in integrating security features into these emerging protocols. Overall, the TCP/IP protocol suite will be significantly less vulnerable by the time IPv6 is fielded.

The IPv6 protocol suite will be technically secure, but there is a nontechnical aspect of Internet security that must be considered in relation to the tactical internet. Once the security features of IPv6 are fully defined, they will be well understood and open to inspection by the entire Internet community. On one hand it is desirable to have core security features that can be tested, validated and implemented by all designers, devices and applications. On the other hand it is dangerous to rely on security features that can be easily examined in detail by the enemy. Fortunately the Internet security architecture [Atkinson,95] does not mandate the use of a specific encryption algorithm. The security architecture does require that all IPv6 implementations *support* the MD5 hash algorithm,

which is widely used in computer security products to compute message digests for authentication and integrity checks. In choosing the IP layer security features to implement in its tactical internet, the Marine Corps must balance the need for compatibility with commercially available equipment and software against the need to protect tactical communications from hostile sources who may be experts in Internet technology. On balance, this open approach to specification and validation leads to stronger protocols, strong encryption configuration options and a more secure infrastructure.

J. TRANSITION MECHANISMS FOR IPV6

1. Transition Overview

The IETF IPng Working Group began development of IPv6 with transition planning at the top of their agenda [Bradner,96a]. The working group realized that for IPv6 to succeed, smooth and incremental transition for the huge installed base of IPv4 equipment and software must be accommodated. Previous attempts to make large-scale protocol transitions had failed due to poor transition planning. A case in point was the U.S. Government's plan to force all of its networks to Open System Interconnect (OSI) protocols [Hinden,95a]. Therefore the IETF planned for a lengthy but deliberate migration from IPv4 to IPv6.

The IETF defined three technical mechanisms to facilitate coexistence of IPv4 and IPv6 in the same internet. These can be summarized as:

- Dual-Stack operation: routers and hosts implementing support for both IPv4 and IPv6 simultaneously.
- IPv6 over IPv4 tunneling: hosts and routers encapsulating complete IPv6 packets as data inside IPv4 packets for transmission over IPv4-only portions of the network.
- IPv4 addresses mapped into IPv6 address space: the IPv4 address can be represented in the rightmost portion of an IPv6 address format (as discussed in Section E above) to facilitate IPv4-IPv6 gateway translations.

2. Dual-Stack Transition Approach

Running both protocols on each node is the most straightforward method of transition and ensure complete interoperability with all other IP nodes. IPv6 nodes running dual protocol stacks can be added to the network without disrupting the in-place IPv4 infrastructure. A disadvantage of this approach is that dual-stack protocol software requires nearly twice the computing resources required for single-protocol operation. Furthermore routers must support both IPv6 and IPv4 to preclude the use of inefficient "tunneling."

Dual-stack nodes have both IPv6 and IPv4 addresses. The IPv6 address can be formed by placing the IPv4 address in rightmost portion of the IPv6 address. (This convention is convenient, but not required). The protocol stack used for a particular communication is determined by the capabilities of the destination host. IPv4 hosts talk to IPv4 hosts; IPv6 hosts talk to other IPv6 hosts. The protocol version being used by the destination host is obtained from the domain name system (DNS) (which itself must be upgraded to handle IPv6 addresses). Routers with both IPv4 and IPv6 protocol stacks will function just like mixed protocol routers do today. If the networks routers do not support both IPv4 and IPv6, packets must be tunneled as described in the next section. [Bradner,96a]

Regardless of the migration strategy employed by the Marine Corps, some dual-stack nodes will be required. Just as electronic mail gateways are required to translate among the myriad types of e-mail, protocol gateways will be needed to translate between IPv4-only and IPv6-only portions of the network.

3. IPv6 over IPv4 Tunneling

IPv4-only routers cannot route IPv6-only packets. Tunneling provides a way for IPv6 hosts to communicate with each other using a predominantly IPv4 infrastructure. The IPv6 hosts must also have IPv4 addresses in order to use this method of communication. Tunneling is accomplished by encapsulating a complete IPv6 packet as

the data payload inside an IPv4 datagram. The network treats the datagram like a normal IPv4 datagram until it reaches an IPv6-capable node where the IPv6 packet is extracted and examined. In practice, tunneling of IPv6 can be host-to-host, router-to-router, host-to-router or router-to-host.

Tunneling IPv6 over a predominantly IPv4 infrastructure negates much of the value added by IPv6. Until intermediate routers support IPv6, the quality of service, mobility and security features of IPv6 are not available to the network's end users. Tunneling must be viewed as an expedient mechanism to be employed in situations where no other solution is possible.

4. IPv4 Addresses Encoded in IPv6

IPv4 addresses can be mapped directly into the IPv6 address space. This powerful transition mechanism allows an IPv6 host to communicate in a limited way with an IPv4-only host using a protocol-translating gateway. The IPv6 host forms an IPv6 address directly from the IPv4 address of the destination. An IPv6-to-IPv4 gateway can interpret the address directly and simply forward the data in an IPv4 datagram. The same process is used in reverse when an IPv4 host needs to communicate with an IPv6 host. This mechanism also makes it simple to change addresses for an IPv4 host that is upgraded to IPv6.

K. IMPLICATIONS OF IPV6 FOR THE TDN ARCHITECTURE

IPv6 makes significant improvements over IPv4 in addressing, multicast, mobility, quality of service and security. These enhanced features are needed for tactical internetworking in the next century and must be included in the long-term tactical internet architecture. However, basing the design of TDN entirely on IPv6 is not prudent because significant deployment and testing of IPv6 implementations remains to be accomplished. Therefore it is recommended that the TDN design proceed based on the proven capabilities of IPv4 and be influenced by expected IPv6 improvements.

Several aspects of the tactical internet architecture require special consideration for the effects of IPv6. The tactical IP addressing plan must incorporate features that will facilitate the eventual integration of IPv6 autoconfiguration and hierarchical routing. This might involve explicit support for the current versions of Dynamic Host Configuration Protocol (DHCP) [Droms,93] and Classless Inter-Domain Routing (CIDR) [Fuller,93]. Of course, utilization of IP Multicast [Deering,89] can be incorporated not only in TDN but also in tactical end-system software applications. A preliminary strategy for employing IPv6's mobility (and IPv4's Mobile IP) and QoS features within the tactical internet must be developed to ensure that TDN's design does not preclude incorporation of these features as they become available. Finally, the IP security architecture [Atkinson,95] options are available now and can be implemented in TDN [Bruno,96]. An integrated TDN security architecture is needed to define the role of IP-layer security features in the tactical internet.

L. SUMMARY

IPv6 is a necessary and natural step in the evolution of the Internet Protocol as an open system network bearer service. IPv6 retains the simplicity and robustness that makes IPv4 so appropriate for tactical networking. The quality of service, multicast and security features added to IPv6 are also necessary to support the emerging technology trends that will affect the Marine Corps tactical internet. Although some aspects of IPv6 are still in the formative stages, IPv6 is on track to become an Internet Standard and commercial software products based on IPv6 will be available by the time the Tactical Data Network (TDN) is fielded. Nonetheless, basing the design of TDN solely on IPv6 is not prudent due to the significant IPv6 deployment and testing that remains. IPv4 is here now and it works. Therefore the design of TDN must proceed based on IPv4 and must include provisions for incorporating the improvements of IPv6. The Marine Corps and the other services must also formulate migration strategies now to ensure a smooth and properly timed transition from IPv4 to IPv6.

VII. AN IP ADDRESS ALLOCATION PLAN FOR THE TACTICAL DATA NETWORK

A. INTRODUCTION

1. Purpose of This Address Plan

The tactical IP addressing plan presented in this study is intended to serve as a baseline IPv4 address allocation architecture for the Tactical Data Network (TDN). Tactical Data Network equipment will be employed by every Fleet Marine Force (FMF) unit battalion-level and above [MCCDC,95a]. Many communications personnel across all echelons will be involved in establishing and maintaining the tactical internet for field exercises and operations. A common frame of reference for allocating and assigning IP addressing is needed to preclude a free-for-all of disparate, inefficient and complex addressing schemes. Communications personnel who are not expert in IP network planning can use this plan to set up basic addressing structures for their units. Finally, this plan identifies the number of IPv4 addresses that must be obtained by the Marine Corps in order to ensure that TDN can be employed to the fullest of its capabilities.

2. Guiding Principles

The TDN addressing plan recommended in this study is based on operational requirements. Addresses were allocated on the basis of both the current need for IP addresses and the projected future growth of IP address requirements. Several overarching precepts guided the development of the plan. In particular the TDN addressing plan must:

- Be simple to understand and implement by people who are not experts in TCP/IP addressing/routing.
- Accommodate future growth of TDN IP address requirements.
- Be usable regardless of the specific IP networking equipment utilized in TDN.
- Keep unclassified addresses separate from classified addresses.

3. Assumptions

TDN will not be fielded until the 1999-2000 timeframe and many questions regarding its concept of operations remain unanswered. Therefore, several assumptions were made in order to include a useful degree of detail in the tactical IP addressing plan. These design assumptions can be summarized as follows:

- That the Marine Corps will not radically alter its tactical organizational structure (MAGTF) between now and 2000.
- That Marine Corps doctrine for MAGTF command and control structure and communications connectivity will remain consistent for the near term.
- That potential future growth of the number of nodes connected to TDN is accounted for.
- That the tactical internet will operate in a SECRET-high security mode, and data traffic of other classification levels will be tunneled across the SECRET network as needed.
- That the TDN program will receive full funding and will be fielded in accordance with the current distribution plan [MARCORSYSCOM,95a].

Future variations in these design assumptions are not likely to invalidate the addressing plan, but may require some plan modifications.

4.Limitations

The TDN IP addressing plan presented in this study is notional and not doctrinal. The plan is intended to serve as a foundation upon which a standard Tri-MEF tactical internet addressing plan can be built. Such a Marine Corps-wide standard operating procedure (SOP) requires substantial review and comment from the entire Fleet Marine Force. Although some communications officers and data systems officers from the FMF contributed their ideas to this plan, the FMF as a whole has not yet been afforded the opportunity to officially review it. The staffing of the TDN IP addressing plan by the TDN Project Office is recommended future work.

The IP addresses allocated in the TDN IP addressing plan proposed in this thesis have not yet been obtained from the military Internet Protocol addressing authority (DoD

NIC). Therefore, substantial changes to the plan may be necessary if sufficient numbers of class C addresses cannot be obtained for TDN. Nonetheless, the goal of the study was to identify the IP addresses *required* for TDN, not to fit an IP address assignment plan to an already existing group of IP addresses. Finally, many details are still unknown about what the Marine Corps' tactical internet will look like when it is fielded. In particular, the physical topology of the network is nearly impossible to determine. For this reason address assignments for most units were left in a generic form that is open to change as greater detail becomes available. Given that the TDN architecture will be diverse and evolve over time, these limitations on future knowledge can optimistically be considered strengths when designing an adaptable tactical network.

B. OVERVIEW OF THE TDN IP ADDRESS ALLOCATION PLAN

The IP addressing plan proposed here is designed to meet currently projected needs of the tactical internet as well as future requirements. This section describes the plan and discusses the technical issues considered in the plan's development.

1. Number of IPv4 Addresses Required

The IPv4 addresses required for a notional Marine Expeditionary Force (MEF) are shown in Table 7.1. A fully deployed MEF requires 128 class C addresses for use on the SECRET tactical internet (connected to SIPRNET) and 64 class C addresses for use on the UNCLASSIFIED tactical internet (connected to NIPRNET). All (or at least most) of these addresses will need to be contiguous for maximum routing efficiency. The number of addresses under the "MEF" heading in Table 7.1 include IP addresses allocated to the Marine Force Component Commander (MARFOR) and the Marine Expeditionary Units (MEUs) within the MEF's area of responsibility. The total numbers of IP addresses required for TDN employment throughout the Marine Corps are listed in Table 7.2. These tables are summaries, with design details and future growth considerations detailed in this chapter. Appendix A contains the detailed TDN tactical IP address allocation plan.

Address Type	MEF	Division	Air Wing	FSSG	Total
SECRET Class C	32	32	48	16	128
UNCLAS Class C	16	16	16	16	64

Table 7.1 IP address requirements for a notional Marine Expeditionary Force.

UNIT	Class C SECRET	Class C UNCLASSIFIED
I MEF including 3 MEUs	112 12	57 3
II MEF including 3 MEUs	112 12	57 3
III MEF including 1 MEU	112 4	57 1
MARFORLANT including contingency JTF cell	4	4
MARFORPAC including contingency JTF cell	4	4
Marine Corps Reserve Forces	112	57
FMF Totals	**484**	**243**
Total Class C Addresses for TDN	727	

Table 7.2 Total IPv4 class C address requirements for the Fleet Marine Force using current projections. Additional growth projections appear in Table 7.4.

2. Global Uniqueness of TDN IP Addresses

All of the IPv4 addresses used in the Tactical Data Network must be obtained from and registered with the Department of Defense Network Information Center (DoD NIC) [DISA,96b]. The DoD NIC will ensure that all IP addresses allocated to TDN are globally unique (i.e. not registered to any other user in the global Internet, NIPRNET, or SIPRNET). **The importance of obtaining globally unique addresses for the tactical internet cannot be overstated.** In the previous chapter it was explained that every host in an internetwork must have an IP address that is unique within that internet. It is unwise to assume that *any* network will never be connected to some universal internetwork like the global Internet. Unclassified tactical networks will certainly be

connected to the Internet in some way. However, classified networks may also connect to global classified internets such as the SIPRNET. The global "infosphere" described in *C4I for the Warrior* [Joint Staff,93] will be reachable by every warfighter at every level of command using whatever computing terminal he happens to have. Similarly as multilevel security (MLS) products make their way into the tactical networking environment both classified and unclassified platforms will share the same network infrastructure. Adhering to IETF addressing standards and recommendations will also simplify eventual migration to IPv6. Therefore TDN must have globally unique addresses to ensure a clear migration path into the next century.

3. Technical Considerations in Developing the Address Plan

a. Routing Considerations

The TDN tactical IP addressing plan is designed to make use of the Classless Inter-Domain Routing (CIDR) address aggregation scheme that was introduced in Chapter V. CIDR makes it possible to represent a block of consecutive class C IPv4 addresses as a single network number. Therefore, instead of advertising individual routes for each network, routers only need to advertise one route for the entire group of networks. This aggregation of information greatly reduces both the computational load on routers and the amount of network bandwidth consumed by routing overhead.

Classless Inter-Domain Routing (CIDR) [Fuller,93] is fully supported by the *Open Shortest Path First version 2* (OSPFv2) [Moy,94] routing protocol which is the Marine Corps' standard interior gateway routing protocol [MCCDC,95b]. OSPF is called an "interior gateway" protocol because it performs routing within an *autonomous system*, i.e. a group of routers using the same protocol and under the control of a single network authority [Comer,95]. Classless Inter-Domain Routing (CIDR) between autonomous systems is performed using "exterior gateway" protocols such as the Border Gateway Protocol version 4 (BGP4), which is also a Marine Corps standard [Rekhter,94]. In the context of the tactical internet, each Marine Expeditionary Force (MEF) is an

autonomous system. Therefore OSPF can be used as the basis for constructing the addressing architecture of the MEF.

Besides the IP addressing structure used, the key network architectural issue that needs to be defined when using OSPF is the definition of *routing areas* [Cisco,95b]. Routers belonging to an OSPF area maintain detailed knowledge about that area's network topology and must recalculate routes whenever the topology changes. Routers outside the area are given only summary information (CIDR) about the area topology on a periodic basis (about every 30 minutes). In order to use the computationally intensive OSPF in the rapidly changing network topology like the tactical internet, routing areas need to be kept small. Experts in the field recommend that no more than 50 routers be assigned to a single area [Cisco,95b]. The areas must be connected by a *backbone* that is stable and has redundant communications. Using these criteria the Marine Division, Marine Air Wing, Force Service Support Group and MEF Command Element were chosen as routing areas for TDN. The logical OSPF routing topology is depicted in Figure 7.1.

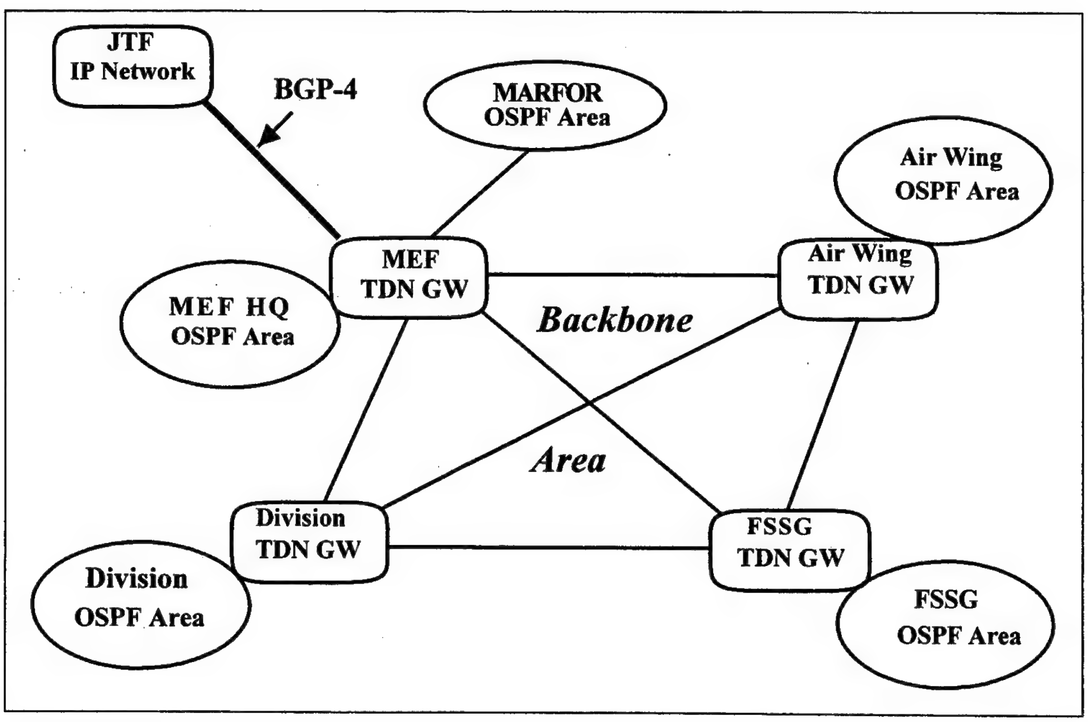

Figure 7.1 Logical OSPF routing topology in the Marine Corps tactical internet.

Each major command (MEF Command Element, Division, Wing, FSSG) is designated an OSPF *routing area*. Additionally, the Marine Forces Component Command (MARFOR) is designated an OSPF area. The TDN Gateways (GW) in the MEF are interconnected via the tactical communications architecture and form the OSPF *backbone area*. The routers in the TDN Gateways exchange summary information about the OSPF areas they serve. The MEF TDN Gateway connects to the joint tactical internet using the BGP-4 protocol. The TDN tactical IP addressing plan is constructed such that network addresses within each OSPF area can be summarized by each TDN Gateway as a single network route.

b. Subnetting Use Minimized

Although OSPF supports variable length subnetting, subnetting was avoided wherever possible in the recommended TDN address plan. Subnetting is administratively intensive and inherently prone to error. Further, specifying subnet numbering in a standardized plan greatly restricts the flexibility afforded to local network managers in adapting solutions to their particular situations. However there are instances in which subnetting was the only reasonable alternative to wasting address space. In those cases where subnets are needed, variable-length subnets have been employed to avoid overly fragmenting the total address space. It is permissible in OSPF and CIDR to define a *subnetID* of any length because every network address carries with it a 32-bit subnet bit mask which explicitly informs the router of the *subnetID*.

The fact that subnetting was not used extensively in the development of this plan does not mean it cannot be done. Class C addresses are used in the recommended TDN addressing plan because they are easier to obtain from the NIC than class B addresses. Indeed detailed justifications are now required to obtain any of the remaining class B addresses. Furthermore, class C addresses will function in any network running any type of IP routing protocol, even if subnetting is not supported. Since *Classless* Inter-Domain Routing was used as the basis for this plan, a class B address might be substituted for the

group of class C addresses that were recommended. Since an address's *class* is ignored when using CIDR, this kind of substitution has no effect on the routing in the network.

c. Network Hardware Considerations

Every effort was made to avoid linking the addressing allocation plan too closely with networking hardware. The Tactical Data Network (TDN) is still an evolving system. Details of the actual hardware that will be integrated into TDN are not currently specified. In any case such details are not critical inputs to the address plan. TDN is a modular system and any of its components can be replaced using equivalent items without greatly affecting the rest of the system. For example, the current TDN specification states that each TDN Server will have four 12-port LAN hubs [MARCORSYSCOM,95c]. This specification was not used as an addressing criterion because larger hubs might easily be substituted by the time TDN is fielded. Instead address allocation was based on anticipated requirements of the FMF. Thus the address plan is grounded in reality. The proposed TDN fielding plan was used to determine which units will actually have networks as well as to gauge the general size and topology of those networks.

The tactical internet of the future will be populated with communication devices that are not specifically part of the Tactical Data Network (TDN) system or the tactical data systems discussed in Chapter IV. Handheld computing devices (such as the Marine Corps Digital Automated Communications Terminal or DACT) and remote sensors are just two examples of the types of equipment that might be connected to the tactical internet. Every such device must be uniquely identified by the network, therefore every such device must have an IP address. There is also a trend toward integrating network management capability (i.e. support for the Simple Network Management Protocol or SNMP) in all kinds of electronic devices. Within several years this trend will extend to radios and many other types of communications equipment. In the tactical internet of the 21st century it is possible that SNMP-manageable devices will outnumber tactical users. This trend was carefully considered in the development of the TDN address plan. Units

with large numbers of electronic devices were allocated enough addresses to accommodate this type of IP address requirement.

C. BASIC IP ADDRESS ALLOCATION/ASSIGNMENT SCHEME

One of the TDN Project Office aims in sponsoring this study is to develop a standard tactical IP addressing scheme for TDN. Therefore a basic template (Table 7.3) was developed for the TDN server, which is intended primarily to connect end users to the tactical internet [MARCORSYSCOM,95c]. The TDN tactical addressing plan allocates at least one class C network number to each FMF unit which has a TDN server. Thus, the generic address assignment template shown in Table 7.3 is a breakdown of a single class C address. The goal of the template approach is to assign standard IP addresses to network services and devices that are common to most TDN LANs. For example, every Web server is assigned IP address number *N.N.N.12* (where "N.N.N" represents the class C network address). Although several well-known network services (i.e. DNS, e-mail server) might be hosted on the same workstation, such a configuration is not required and was not assumed to be the norm. Therefore, a separate IP address was assigned to each well-known network service in order to allow local network administrators greater predictability when configuring those services.

The convention of assigning *hostID #1* to the network router was maintained. Several other addresses were also allocated to the router to allow some flexibility in assigning the router such services as the Mobile IP home agent. *HostID #6* is reserved for a personal computer (PC) network file server that might reside on the LAN. *HostID #7* is reserved for the local Defense Messaging System (DMS) Message Transfer Agent (MTA). *HostID #8* is reserved for multilevel security devices that might be incorporated into TDN, such as the Secure Network Server (SNS) and the Motorola Network Encryption System (NES). Addresses *N.N.N.9-12* are reserved for well-known Internet services, and addresses *N.N.N.13-30* are allocated to TDN ancillary hardware components.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
FMF Unit	N.N.16.0	N.N.16.0	N.N.16.1-5	TDN router
			N.N.16.6	LAN file server
			N.N.16.7	DMS MTA
			N.N.16.8	SNS/NES/INE
			N.N.16.9	DNS server
			N.N.16.10	DHCP server
			N.N.16.11	SMTP mail server
			N.N.16.12	Web server
			N.N.16.13	TDN management workstation
			N.N.16.14-16	UPSs
			N.N.16.17-20	External drives/RAID
			N.N.16.21-24	TCIMs
			N.N.16.25-30	TDN repeaters
			N.N.16.31-33	reserved
			N.N.16.34	main TCO workstation
			N.N.16.35-254	LAN users (220 total)
			N.N.16.255	network broadcast

Table 7.3 Example of the basic TDN IP address assignment within an FMF unit.

Addresses *N.N.N.31-33* are reserved for future subnetting (if necessary). It is expected that subnets in the tactical internet will not be smaller than 30 *hostIDs* (except for point-to-point link subnets). Thirty-user subnets are created by using the first three bits of the *hostID* portion of the class C IP address to indicate the *subnetworkID*. This creates subnets that are numbered: *0,32,64,96,128,160,192,* and *224*. The first *hostID* in each subnet is assigned to the router, and the last *hostID* is the subnet's broadcast address. For example, in 3-bit subnetting *N.N.N.31* is the broadcast address for subnet number *N.N.N.0*. The network number of the next subnet is *N.N.N.32* and address *N.N.N.33* identifies the router port that is connected to subnet *N.N.N.32*. Therefore, these three numbers are reserved in the standard template.

In most units the remainder of the *hostIDs* are reserved for end users. IP address *N.N.N.34* is reserved for the unit's primary Tactical Combat Operations (TCO) workstation. This was made a standard address because every FMF unit that will have

TDN will also have at least one TCO terminal [MCTSSA,95]. Further partitioning of the *hostID* portion of the IP address space is assumed to be unit/network dependent. Further, many of the tactical data systems that will connect to TDN have not published equipment fielding plans. It is also likely that dynamic IP address assignment will become the norm for individual host addressing. The actual IP addresses of end systems will be less important than the binding between user-understandable directory services (X.500) and naming systems (DNS).

D. FUTURE GROWTH AND ADDRESS SPACE ALLOCATION

A consistent trend in internetworking is that growth exceeds expectations. Price/performance improvements in computer hardware are 10 percent per month, doubling each year. Global growth of the Internet averages approximately 15 percent per month, which equates to a doubling in size every five to six months. A prudent network design considers these long-term sustained exponential growth rates, and the accompanying technological improvements which drive them, in addition to predicted operational requirements. Significant allowances for growth are already incorporated in the address plan assignment templates contained in Appendix A. Nevertheless, other future growth possibilities must be considered.

The address plan proposed in this study assumes that TDN will extend down to company level. Specific 30-user subnet addresses are assigned to companies and batteries in the armored vehicle, artillery, and light anti-air defense battalions. In other units of the MEF, sufficient IP addresses are also provided so that networked devices at the company level can be assigned at the discretion of the battalion/squadron-level commander. If more than 30 communications devices within a company are internetworked with TDN, the addressing space requirements specified in this plan must be increased. For example, extending TDN to every individual Marine in the MEF might require that the TDN IP address space be increased by a factor of four.

Significant routing benefits accrue in IPv4 when using a contiguous address space. For that reason, and for sustained exponential growth reasons, a larger address space must

be reserved for TDN than is needed to meet currently projected requirements. A larger IPv4 address space also provides for a longer transition period if IPv6 deployment is delayed. Table 7.4 extends the totals provided in Table 7.2 to provide for unforeseen growth in the size of the tactical internet. Minimum recommended and recommended address spaces are listed.

Class C Address Requirements (SECRET plus UNCLASSIFIED)	Current	Growth Factor	Total Projected
Current TDN Requirements	727	1	727
Minimum Recommended	727	2	1,454
Minimum Recommended with TDN extended to individual Marine level	727	4	2908
Recommended IPv4 Address Space to be Reserved for TDN			2908

Table 7.4 Total IPv4 Class C address requirements for the Fleet Marine Force Tactical Data Network, accounting for unforeseen growth.

The Marine Corps Tactical Data Network (TDN) Project Office needs to ensure that the military IP addressing authority (DoD NIC) reserves adequate contiguous IPv4 address space to meet approved recommendations. The cost of reserving too many addresses (inefficient address assignment) is trivial. The cost of reserving too few addresses is potentially devastating. An address shortfall may require massive renumbering of the tactical internet, or in the worst case may result in some end systems not being able to communicate across the network at all.

E. SUMMARY

The Tactical Data Network IP address allocation plan presented in this study is consistent with current best practices in the IP internetworking field. It provides enough address space for current tactical IP address requirements and also provides room for future growth. With the advent of Internet Protocol version 6, address *space* will become less of a concern, but address *hierarchy* will continue to be critical to routing efficiency. CIDR is the prototype for next generation hierarchical routing, and OSPFv2 is currently

being upgraded to work with IPv6. By employing Classless Inter-Domain Routing (CIDR) and OSPFv2 in TDN, the Marine Corps positions itself to make a smooth transition into the next generation internetworking environment. Implementation of this tactical IP addressing plan is vital to the overall Tactical Data Network IPv6 migration strategy.

VIII. MIGRATION TO INTERNET PROTOCOL VERSION 6

A. INTRODUCTION

When the Tactical Data Network (TDN) is fielded, portions of the global Internet may already be transitioning from IPv4 to IPv6. Integrating transition planning into the TDN architecture will ensure that TDN is a viable internetworking backbone for the Marine Corps tactical internet in the next century. This chapter discusses some of the issues the Marine Corps must consider when formulating its IPv6 migration strategy.

B. FACTORS FORCING THE MIGRATION TO IPV6

Exhaustion of IPv4 address space is the primary factor is forcing the move toward IPv6 in the global Internet [Hinden,95a]. The tactical internet's need for IPv6 is somewhat different. Address space will not be a problem for the Tactical Data Network (TDN) if the Marine Corps implements the tactical IP addressing plan proposed in this study. IPv6's added functionality in supporting multicast, mobility and security are certainly needed by TDN, but many of those capabilities will be available as extensions to IPv4. Rather, the tactical internet's migration to IPv6 will be driven by the quality of service (QoS) requirements of next generation applications software. Multimedia, collaborative planning and distributed simulation applications will require QoS guarantees in order to operate in the low-bandwidth intermittent communications environment of the tactical internet. These QoS requirements cannot be met consistently by IPv4. IPv6 is the only potential successor to IPv4 that is an open systems standard, is independent of hardware, and also enjoys widespread support among network research communities and commercial vendors. IPv6 is hand-crafted by the global Internet community itself and it is unlikely to falter. Therefore the Marine Corps must adopt the position that eventual migration to IPv6 is a necessary step in the evolution of the tactical internet.

C. IPV6 DEPLOYMENT CONSIDERATIONS

1. Introduction

This section addresses the "how" of upgrading to IPv6. It is unreasonable to expect that IPv6 will be implemented everywhere at once. IPv4-only nodes and networks will coexist with dual-protocol (IPv4 and IPv6) and IPv6-only nodes and networks for years. This will be true of both the global Internet and the tactical internet. Therefore the deployment of IPv6 in the tactical internet must be carefully planned to ensure minimal disruption of the existing IPv4 infrastructure as well as backward compatibility with networks and nodes that do not upgrade to IPv6.

2. Physical Actions Required to Upgrade to IPv6

Introduction of IPv6 into the existing IPv4-based tactical internet requires only software changes. No TDN or end-system (host) hardware will have to be modified to accept IPv6. Routers are upgraded to IPv6 by adding new IP layer software, IPv6-capable routing software, and IPv6-capable network management software to the routers' protocol stacks [Bound,96]. Even so, overdue unsupported router replacements may be occasionally necessary.

Host upgrades are somewhat more complex. In addition to IP layer software, hosts have transport layer and application layer software that must be upgraded to work with IPv6. If TCP/IP protocol software is built into a host's operating system (as is the case for hosts running UNIX and WindowsNT), upgrading to IPv6 may necessitate the replacement or recompiling of the host's operating system [Trinity,95]. For example, a typical tactical internet host running the GCCS common operating environment (COE) might have all of the following protocol software: Transmission Control Protocol (TCP), User Datagram Protocol (UDP), File Transfer Protocol (FTP), Domain Name System (DNS), Simple Mail Transport Protocol (SMTP), and TELNET [MARCORSYSCOM,94]. All of these protocols and applications must be modified in some way to accommodate IPv6 [Bound,96]. In general any protocol or application that embeds IP addresses must be modified to recognize and utilize IPv6's 128-bit address.

Applications that will utilize the multicast, mobility, quality of service and security features of IPv6 will require more extensive modification [Bound,96]. However applications that are designed now to use the IP Multicast [Deering,89], Mobile IP [Perkins,96b] and IP security [Atkinson,95] extensions to IPv4 are expected to require less modification than those applications that have no support for these protocols. Finally, of course every node that is upgraded to IPv6 must be assigned at least one IPv6 address. [Bound,96]

Nodes that run dual-protocol stacks (IPv4 and IPv6) require transition software. For example, dual-stack nodes must have a protocol selection mechanism that enables higher-layer software to choose the appropriate IP layer protocol (IPv4 or IPv6). In practice vendors will probably bundle IPv4 and IPv6 in an integrated dual-stack software package, thus making IPv6 upgrade much simpler. [Bound,96]

Upgrading the tactical internet to IPv6 will not be a trivial undertaking. Steps can be taken now to reduce the burden of the transition. Application layer software modification and re-engineering will be minimized if IPv6 is considered in the original design. For example, tactical applications must not make assumptions about the IP address format. Further, tactical applications must be designed to utilize the enhanced multicast, mobility and security features of IPv4. These actions will result in significant savings in complexity and cost when the transition to IPv6 commences.

3. Recommended Method of IPv6 Deployment

It is recommended that IPv6 be deployed in the tactical internet incrementally, beginning with TDN routers and then extending to end systems as needed. Interoperability and continuity of service must be maintained throughout the introduction of IPv6, thus ruling out an "all-at-once" transition. Similarly the Marine Corps tactical internet cannot remain an IPv4-only "island." It is technically possible to retain IPv4 internally and connect to IPv6 networks using IPv4-to-IPv6 translation gateways. However such an approach denies Marine Corps users the needed features of IPv6 and will not support the future TDN internetworking requirements. Incremental deployment

of IPv6 will ensure the stability of existing IPv4 infrastructure and provide the flexibility to transition to IPv6 on a user-driven schedule.

TDN routers must be the first elements of the tactical internet to be upgraded to IPv6. Routers are crucial to the delivery of IPv6's QoS, multicast, and mobility services. Once TDN's routers are running IPv6, hosts that are upgraded will have access to IPv6 services regardless of the hosts' location in the network. Further, to ensure that the IPv4 infrastructure is not disrupted by the transition to IPv6, all TDN routers must be configured as dual-stack nodes.

Concurrent with the upgrade of routers, IPv6 support must be added to DHCP and DNS servers. These services are important for IPv6 host configuration and communication. With the basic IPv6 infrastructure support in place, end systems can upgraded to IPv6 as needed. Initially, most end systems will also have to be configured as dual-stack nodes to facilitate interoperability. As IPv6-only hosts become more common, IPv4-to-IPv6 translating gateways will be required.

The minimalist view of IPv6 transition is that only those hosts which absolutely need IPv6 should be upgraded. Any cost savings that might result from this approach will be negated by the added complexity of a hybrid networking environment. Isolated IPv6 nodes make network management more difficult and reduce the network's transparency and flexibility for end users. For example, IPv6-only applications must not be restricted to only one or two hosts in a command center. The whole idea behind the common operating environment (COE) is that end users are able to execute tactical applications on any COE platform. Therefore when upgrading a local-area network (LAN) to IPv6, every node on the LAN segment must be upgraded to a dual-stack configuration.

4. IPv6 Deployment Summary

An incremental approach must be taken to the deployment of IPv6 in the tactical internet in order to ensure interoperability and backward compatibility. Upgrading the IP software in the TDN routers first will ensure that critical IPv6 capabilities are available

throughout the network to IPv6 hosts that need them. Maintaining dual protocol (IPv4 and IPv6) stacks on all TDN routers is necessary to allow IPv4 hosts to be upgraded incrementally as needed.

D. ISSUES IMPACTING TDN MIGRATION TO IPV6

1. Introduction

Many aspects of both IPv6 and the Tactical Data Network (TDN) are still evolving. This section discusses several issues that will have a significant impact on both the timing of IPv6 migration and the viability of the TDN tactical IP addressing architecture proposed in this study.

2. Employment of IPv6 Address Autoconfiguration

The tactical IP address plan proposed in this study is designed to facilitate an orderly transition to IPv6. For example, changing TDN IPv4 addresses into IPv6 addresses might be as simple as adding a six double-octet prefix as shown in Figure 8.1.

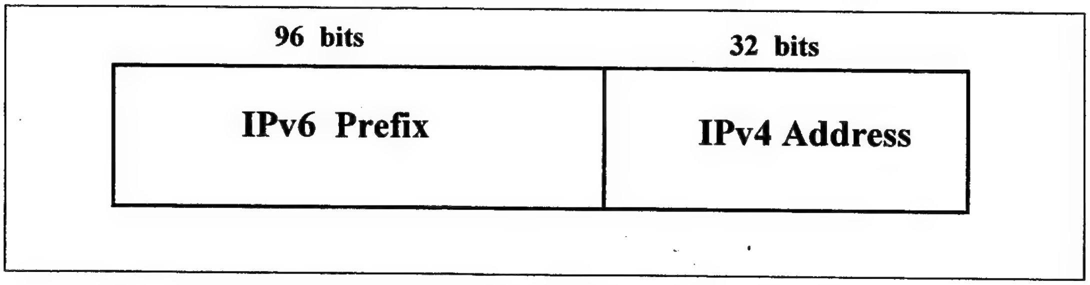

Figure 8.1 Forming a 128-bit IPv6 address by attaching an IPv6 prefix to an IPv4 address.

This procedure preserves the topological and hierarchical structure of the TDN tactical IP addressing plan. However the way in which IPv6 address autoconfiguration is employed may lead to the renumbering of TDN.

Two methods of IPv6 autoconfiguration were discussed in Chapter VI: *stateful* and *stateless*. Stateful autoconfiguration uses the same Dynamic Host Configuration Protocol (DHCP) [Droms,93] that will be used in the TDN to assign IPv4 addresses to

hosts. Therefore employment of stateful IPv6 autoconfiguration will provoke few changes to the TDN addressing plan. A host employing stateless IPv6 autoconfiguration combines information provided by a local router with information the host itself already knows (such as its Ethernet hardware address) to form an IPv6 address [Thomson,95]. Since hardware addresses have no topological significance, IPv6 addresses created in this manner are only related to addresses of other hosts on the same subnet by the IPv6 prefix. In such a case the original IPv4 address structure of the network pertaining to host assignment conventions will be of no use in routing.

One approach to this issue is to use only the stateful method of IPv6 address autoconfiguration in TDN, but this policy is too restrictive to satisfy the dynamic needs of tactical internet end users. A better approach is to align IPv6 address prefixes with the structure of the TDN tactical IPv4 addressing plan, permitting effective stateful and stateless autoconfiguration. The latter option requires that an assignment allocation be thought out well in advance of IPv6 deployment. This will ensure that the correct IPv6 address blocks can be obtained from the IPv6 address assignment authority.

3. Mobile IP Development

The eventual solution for IPv6 mobility support will have a significant impact on the viability of the TDN tactical IP addressing architecture. The draft proposals for Mobile IP [Perkins,96b] and IPv6 mobility support [Perkins,96a] each require mobile nodes to retain a topologically significant *home address*. Mobile hosts and mobile subnetworks do not require renumbering just because they change their point of attachment to the network. This stabilizes the assignment of IP addresses and simplifies routing, but requires special mobility support in the network. Alternatives to Mobile IP involve dynamic address reconfiguration and dynamic bindings of domain names to IP addresses. Protocols that facilitate dynamic IP addressing [Droms,93] [Rekhter,96a] [Vixie,96] are immature. Therefore it is unclear what the most viable IP layer mobility solution will be. The interconnection between mobility support and the TDN addressing plan is a key issue that must be addressed in the IPv6 migration strategy.

4. Maturity of IPv6 Quality of Service (QoS) Features

Quality of service issues will greatly affect the overall migration of TDN to IPv6. The most important aspects of IPv6 QoS support that impact the IPv6 migration strategy are:

- How applications and higher layer protocols will negotiate QoS with the network.
- How IPv6 will technically enforce QoS guarantees across the intermediate networks.
- How network managers will control/enforce tactical internet QoS and priorities across networks that are "owned" by different military organizations/services.

The QoS negotiation methods supported by IPv6 will determine the extent of the effort needed to upgrade tactical internet applications and router software. For example, if IPv6 QoS will be negotiated by the RSVP protocol [Braden,96], tactical internet designers can ensure that support for RSVP is engineered into TDN system components as well as into end-user applications software.

It remains to be seen how the *flow label* and *priority* fields in the IPv6 packet header will actually be used to guarantee quality of service across disparate physical networks. The integration of IPv6 and ATM QoS features is especially crucial to the IPv6 migration plans for the entire joint tactical internet. ATM is a major part of the midterm joint tactical communications architecture [JIEO,95a] and may be incorporated into the Marine Corps architecture as well [MCCDC,95b]. Therefore stability of the IPv6-over-ATM specifications [Armitrage,96] may be a prerequisite to IPv6 migration.

Finally the management of QoS and priority for data flows that span several subnetworks within the tactical internet is a critical issue that must be addressed. The case that a quality of service requirement exists has already been made in this study. It is good to have the technical capability to enforce quality of service, but a concept of employment for QoS features must also be developed. The IPv6 migration strategy must define how the technical and management aspects of network QoS will be employed once IPv6 is deployed.

5. Integration of IP Layer Security Features

IPv6 security must be addressed long before any migration commences. The *Security Architecture for the Internet Protocol* (IPSEC) [Atkinson,95] extends to both IPv4 and IPv6. Therefore the integration of the basic IP-layer security must be addressed as part of the original TDN design (based on IPv4) [MARCORSYSCOM,95a]. Nonetheless IPv6 will add several new security concerns that are not present in IPv4. IPv6 *anycasting* [Partridge,93] security concerns were discussed in Chapter VI. Security must also be considered in planning the employment of IPv6 quality of service and mobility features. An integrated TDN security architecture is needed that incorporates IPSEC features of IPv4 and also provides for a smooth transition to IPv6.

6. Other Military Services Plans for IPv6 Migration

The Marine Corps tactical internet will be part of the Defense Information Infrastructure (DII) [DISA,95] that is expected to encompass all strategic and tactical networks. Therefore the Corps' IPv6 migration strategy must consider the migration paths being taken by the other military services. None of the other services has yet enunciated an IPv6 migration plan. Therefore the Marine Corps must take the lead in laying out the roadmap to a IPv6-based tactical architecture.

7. Migration Issues Summary

Developers of the Marine Corps' IPv6 migration strategy must address a number of evolving issues. The autoconfiguration and mobility features of IPv6 must be considered in deciding the future direction of the TDN tactical IP addressing plan. The structure of IPv6's quality of service features will impact tactical software application design as well as TDN network management. A TDN security architecture must be developed that defines the role of IP layer security. Finally, in deciding on an IPv6 transition timeline the Marine Corps must consider not only its own needs and the maturity of IPv6, but also the migration plans of the other military services.

E. SUMMARY

The quality of service requirements of next generation tactical software applications will drive the Marine Corps' migration to IPv6. A strategy for transitioning to IPv6 must be mapped out now, and IPv6 compatibility must be considered while architecting and deploying the Tactical Data Network (TDN). An IPv6 upgrade path must be designed into all tactical internet systems in order to avoid costly re-engineering later.

IPv6 must be incrementally deployed in the tactical internet utilizing the dual-stack IPv6 transition mechanism described in Chapter VI. This will ensure both the availability of IPv6 capabilities and backward compatibility with IPv4-only systems.

The timing of the migration to IPv6 will be affected by the maturity of IPv6 as well as by the migration plans of the other military services. The Marine Corps must lead the way in laying the foundation for a joint tactical internet IPv6 migration strategy.

IX. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The Tactical Data Network (TDN) will be the foundation of the Marine Corps' tactical internet for at least the first decade of the 21st century. This tactical internet must be based upon open systems standards that are hardware-independent and commercially available. The internet's infrastructure must enable end users to seamlessly exchange information across disparate physical communications media.

The internetworking needs of the Marine Corps can best be met by the Internet Protocol (IP). Adoption of IP as the centerpiece of the tactical internet architecture is essential to ensure universal interoperability and an open systems evolutionary upgrade path. The Marine Corps gains significant technology leverage by basing its tactical internet on the protocols of the global Internet. The Internet's network research community continues to proactively develop and refine simple, capable and robust protocols to support real-world applications. The importance of the Internet Protocol in the future of universal networking is underscored by this excerpt from "The Unpredictable Certainty: The Information Infrastructure Through 2000" [NRC,96]:

> It would appear at this time that the Internet and its protocols represent the best approach for providing a general service for the support of emerging applications because of the effectiveness with which the Internet protocol serves as a bearer service and the overall architecture functions as an Open Data Network. The current volume of deployed devices using Internet standards, together with observed level of investment in Internet-related products and services, constitutes a unique foundation, one for which there is no alternative now or in any reasonable time frame. For this reason, the steering committee further concluded that specific attention should be paid to ensuring the viability of the Internet, in terms of both enhancing the standards to meet evolving application needs and making sure that networks based on these interfaces are deployed and made widely available as an environment for the innovation of new applications. [NRC,96]

The current version of the Internet Protocol (IPv4) is highly stable and mature, widely implemented and well-understood. IPv4 will adequately support the internetworking demands of the current generation of tactical data systems and software applications. However, the Next Generation Internet Protocol (IPv6) will be needed to fulfill quality of service, security and mobility needs of the next generation of software applications. IPv6 is immature and commercial protocol software implementations are not expected before late 1997. The technical risk associated with IPv6 compels a tactical internet architecture and deployment plan based on IPv4.

Eventually both the global Internet and the tactical internet will migrate to IPv6. Therefore IPv4-to-IPv6 transition planning must be integral to the design and deployment of the Tactical Data Network (TDN), tactical data systems and tactical software applications. Failure to incorporate IPv6 considerations into the tactical internet architecture now may result in major cost, complexity and reliability consequences later.

B. RECOMMENDATIONS FOR FUTURE WORK

1. Implement the TDN Tactical IP Addressing Plan

The IP addressing plan is a key element of the TDN architecture. The addressing plan proposed in this study is based on successful IPv4 protocols (OSPFv2) and best current Internet practices (Classless Inter-Domain Routing) that have a strong connection to IPv6. Implementation of this plan will facilitate a smooth transition to IPv6.

2. Develop an Integrated Security Architecture for TDN

A security architecture is needed that defines the role of each protocol layer in providing security for the tactical internet. The security architecture is essential for planning security product acquisitions and making design decisions. It is also a vital input to the IPv6 migration strategy. This security architecture can be designed using emerging *IPSEC* protocols.

3. Conduct Studies to Determine the True Extent of Next Generation Applications Software Requirements

Since applications will drive the migration to IPv6, it is necessary to quantify the nature of tactical internet quality of service requirements. This might be accomplished through simulations which incorporate real-world data obtained from prototype tactical data systems.

4. Formulate an IPv6 Migration Strategy

The Marine Corps' IPv6 migration strategy must address both the timing and the general method of transitioning the tactical internet to IPv6. More importantly, the strategy must define the architectural elements affected by the IPv6 transition and identify the IPv6 considerations that must be factored into current and planned systems' designs.

5. Establish a Joint Tactical Internet Architecture Working Group

The consensus in DoD is that all future military operations will be joint. A joint working group must architect a tactical internet that provides seamless exchange of data across the entire battlespace.

C. SUMMARY

The Tactical Data Network will revolutionize tactical information transfer in the Marine Corps. A TDN design based on the proven capabilities of IPv4 is sound. IPv6 will be needed to meet emerging requirements, and early planning for incorporation of IPv6's improvements will ensure a viable tactical internet for the next century.

APPENDIX A. PROPOSED TACTICAL IP ADDRESS ALLOCATION PLAN

A. INTRODUCTION

This appendix contains specific detailed information about the address allocation plan outlined in Chapter VII. The tactical IP address plan consists of address assignment tables that are accompanied by brief discussions of how those address assignments were developed.

A notional Marine Expeditionary Force (MEF) is used as the frame of reference for making tactical IP address assignments. The entire MEF is assigned a block of contiguous class C IP network numbers. Each major unit (battalion and above) within the MEF is then allocated an IP address or contiguous range of IP addresses from that block. **The IP addresses listed in this plan are for illustration only and do not represent actual IP network numbers obtained from the DoD NIC**. For clarity separate tables are not shown for every unit within the MEF. In general only one example is shown for each unit type (e.g. infantry battalion).

B. TOTAL IP NETWORK NUMBER ASSIGNMENTS FOR THE MEF

Table A.1 lists the major units within the MEF and the corresponding IP network numbers assigned to each unit. The addresses in Table A.1 are to be used on the classified (SECRET) tactical internet. The total IP address allocations for unclassified addresses are listed in Table A.2. An address range is assigned to each major subordinate element of the MEF (GCE, ACE, CSSE) and the MEF Command Element. The number of addresses in these ranges must be a power of two (i.e. 2,4,8,16,32,64,128...) so that the network address summarization capabilities of Classless Inter-Domain Routing (CIDR) can be exploited. For example, all 32 class C networks within the Marine Division OSPF routing area can be advertised to the rest of the tactical internet as a single network number: *N.N.32.0*. This simplifies both routing and network management. The CIDR summarization model is used throughout the MEF wherever possible.

NAME of MEF UNIT	Number of Class C IP Addresses	Class C IP Address Range
COMMAND ELEMENT (CE)		
Marine Forces Component HQ	2	N.N.0.0-N.N.1.0
First Marine Expeditionary Unit (MEU)	4	N.N.2.0-N.N.5.0
Second Marine Expeditionary Unit	4	N.N.6.0-N.N.9.0
Third Marine Expeditionary Unit	4	N.N.10.0-N.N.13.0
Contingency Joint Task Force (JTF)	2	N.N.14.0-N.N.15.0
Marine Expeditionary Force TDN Gateway	1	N.N.16.0
MEF Main Command Post (COC)	1	N.N.17.0
Communications Battalion	3	N.N.18.0-N.N.20.0
SRIG	1	N.N.21.0
Radio Battalion	1	N.N.22.0
MEF Forward Command Post	1	N.N.23.0
MEF Contingency Addresses	8	N.N.24.0-N.N.31.0
CE Total	**32**	N.N.0.0-N.N.31.0
GROUND COMBAT ELEMENT (GCE)		
Marine Division TDN Gateway	1	N.N.32.0
Division Main Command Post	1	N.N.33.0
Division Forward Command Post	1	N.N.34.0
Division Rear Command Post	1	N.N.35.0
Division Contingency Addresses	2	N.N.36.0-N.N.37.0
Direct Air Support Center (DASC)	1	N.N.38.0
Combat Engineer Bn	1	N.N.39.0
Artillery Regiment	3	N.N.40.0-N.N.42.0
Artillery Battalions (5)	5	N.N.43.0-N.N.47.0
Infantry Regiment	1	N.N.48.0
Infantry Battalions (3)	3	N.N.49.0-N.N.51.0
Infantry Regiment	1	N.N.52.0
Infantry Battalions (3)	3	N.N.53.0-N.N.55.0
Infantry Regiment	1	N.N.56.0
Infantry Battalions (3)	3	N.N.57.0-N.N.59.0
Tank Battalion	1	N.N.60.0
Light Armored Recon Bn	1	N.N.61.0
Assault Amphibian Bn	2	N.N.62.0-N.N.63.0
GCE Total	**32**	N.N.32.0-N.N.63.0

Table A.1 Allocation of classified IP addresses for a notional Marine Expeditionary Force.

NAME of MEF UNIT	Number of Class C IP Addresses	Class C IP Address Range
AVIATION COMBAT ELEMENT (ACE)		
Marine Air Wing TDN Gateway	1	N.N.64.0
Tactical Air Command Center	1	N.N.65.0
Marine Wing HQ	1	N.N.66.0
Marine Wing Support Group	1	N.N.67.0
Marine Air Control Group HQ	1	N.N.68.0
Marine Wing Communications Squadron	1	N.N.69.0
Marine Air Wing Contingency Addresses	2	N.N.70.0-N.N.71.0
Fixed Wing Marine Air Group #1/Marine Air Traffic Control Squadron	1	N.N.72.0
Fixed Wing Marine Air Logistics Squadron #1	1	N.N.73.0
Fixed Wing Marine Wing Support Squadron #1	1	N.N.74.0
Fixed Wing Squadrons	7	N.N.75.0-N.N.81.0
Fixed Wing Marine Air Group #2/Marine Air Traffic Control Squadron	1	N.N.82.0
Fixed Wing Marine Air Logistics Squadron #2	1	N.N.83.0
Fixed Wing Marine Wing Support Squadron #2	1	N.N.84.0
Fixed Wing Squadrons	7	N.N.85.0-N.N.91.0
Rotary Wing Marine Air Group #1/Marine Air Traffic Control Squadron	1	N.N.92.0
Rotary Wing Marine Air Logistics Squadron #1	1	N.N.93.0
Rotary Marine Wing Support Squadron #1	1	N.N.94.0
Rotary Wing Squadrons	5	N.N.95.0-N.N.99.0
Rotary Wing Marine Air Group #2/Marine Air Traffic Control Squadron	1	N.N.100.0
Rotary Wing Marine Air Logistics Squadron #2	1	N.N.101.0
Rotary Marine Wing Support Squadron #2	1	N.N.102.0
Rotary Wing Squadrons	5	N.N.103.0-N.N.107.0
Marine Air Control Squadron #1	1	N.N.108.0
Marine Air Control Squadron #2	1	N.N.109.0
Low Altitude Air Defense Battalion	1	N.N.110.0
Light Antiaircraft Missile Battalion	1	N.N.111.0
ACE Totals	48	N.N.64.0-N.N.111.0

Table A.1 (continued) Allocation of classified IP addresses for a notional Marine Expeditionary Force.

NAME of MEF UNIT	Number of Class C IP Addresses	Class C IP Address Range
COMBAT SERVICE SUPPORT ELEMENT (CSSE)		
Force Service Support Group TDN Gateway	1	N.N.112.0
Force Service Support Group HQ	1	N.N.113.0
Combat Service Support Operations Center	1	N.N.114.0
Supply Battalion (SMU)	1	N.N.115.0
Maintenance Battalion	1	N.N.116.0
Medical Battalion	1	N.N.117.0
Dental Battalion	1	N.N.118.0
Motor Transport Battalion	1	N.N.119.0
Engineer Support Battalion	1	N.N.120.0
Landing Support Battalion	1	N.N.121.0
Combat Service Support Element #1	1	N.N.122.0
Combat Service Support Element #2	1	N.N.123.0
FSSG Contingency Addresses	4	N.N.124.0-N.N.127.0
CSSE Total	16	N.N.112.0-N.N.127.0
MEF Total	128	N.N.0.0-N.N.127.0

Table A.1 (continued) Allocation of classified IP addresses for a notional Marine Expeditionary Force.

NAME of MEF UNIT	Number of Class C IP Addresses	Class C IP Address Range
COMMAND ELEMENT (CE)		
Marine Forces Component HQ	2	N.N.192.0-N.N.193.0
First Marine Expeditionary Unit (MEU)	1	N.N.194.0
Second Marine Expeditionary Unit	1	N.N.195.0
Third Marine Expeditionary Unit	1	N.N.196.0
Contingency Joint Task Force (JTF)	3	N.N.197.0-N.N.199.0
Marine Expeditionary Force TDN Gateway	1	N.N.200.0
MEF Main Command Post (COC)	1	N.N.201.0
MEF Forward CP	1	N.N.202.0
Communications Battalion	1	N.N.203.0
SRIG HQ and Radio Battalion	1	N.N.204.0
MEF Contingency Addresses	3	N.N.205.0-N.N.207.0
CE Total	16	N.N.192.0-N.N.207.0
GROUND COMBAT ELEMENT (GCE)		
Marine Division TDN Gateway	1	N.N.208.0
Division Main Command Post	1	N.N.209.0
Rear Command Post	1	N.N.210.0
Division Forward	1	N.N.211.0
Division Contingency Address	1	N.N.212.0
Combat Engineer Battalion/DASC	1	N.N.213.0
Tank Battalion/LAR Battalion	1	N.N.214.0
Assault Amphibian Battalion	1	N.N.215.0
Artillery Regiment incl 5 Battalions	2	N.N.216.0-N.N.217.0
Infantry Regiment incl 3 Battalions	2	N.N.218.0-N.N.219.0
Infantry Regiment incl 3 Battalions	2	N.N.220.0-N.N.221.0
Infantry Regiment incl 3 Battalions	2	N.N.222.0-N.N.223.0
GCE Total	16	N.N.208.0-N.N.223.0

Table A.2 Allocation of unclassified IP addresses for a notional Marine Expeditionary Force.

NAME of MEF UNIT	Number of Class C IP Addresses	Class C IP Address Range
AVIATION COMBAT ELEMENT (ACE)		
Marine Air Wing TDN Gateway	1	N.N.224.0
Marine Wing HQ/Tactical Air Command Center	1	N.N.225.0
Marine Wing Support Group	1	N.N.226.0
Marine Air Control Group HQ	1	N.N.227.0
Marine Wing Communications Squadron	1	N.N.228.0
Fixed Wing MAG #1 incl MALS/MWSS/MATCS	1	N.N.229.0
Fixed Wing Squadrons	1	N.N.230.0
Fixed Wing MAG #2 incl MALS/MWSS/MATCS	1	N.N.231.0
Fixed Wing Squadrons	1	N.N.232.0
Rotary Wing MAG #1 incl MALS/MWSS/MATCS	1	N.N.233.0
Rotary Wing Squadrons	1	N.N.234.0
Rotary Wing MAG #2 incl MALS/MWSS/MATCS	1	N.N.235.0
Rotary Wing Squadrons	1	N.N.236.0
Marine Air Control Squadrons	1	N.N.237.0
LAAD/LAAM Battalions	1	N.N.238.0
Marine Air Wing Contingency Address	1	N.N.239.0
ACE Total	16	N.N.224.0-N.N.239.0
COMBAT SERVICE SUPPORT ELEMENT (CSSE)		
Force Service Support Group TDN Gateway	1	N.N.240.0
Force Service Support Group HQ	1	N.N.241.0
Combat Service Support Operations Center	1	N.N.242.0
Medical Battalion	1	N.N.243.0
Dental Battalion	1	N.N.244.0
Supply Battalion (SMU)	1	N.N.245.0
Maintenance Battalion	1	N.N.246.0
Motor Transport Battalion	1	N.N.247.0
Engineer Support Battalion	1	N.N.248.0
Landing Support Battalion	1	N.N.249.0
Combat Service Support Element #1	1	N.N.250.0
Combat Service Support Element #2	1	N.N.251.0
FSSG Contingency Addresses	4	N.N.252.0-N.N.255.0
CSSE Total	16	N.N.224.0-N.N.255.0
MEF Total	64	N.N.192.0-N.N.255.0

Table A.2 (continued) Allocation of unclassified IP address for a notional Marine Expeditionary Force.

The assumption was made that the Marine Corps will operate its primary tactical internet at the SECRET security level. Most units will be fielded only one TDN Server which will operate a local-area network at only one classification level. Unclassified network access by these units will be accomplished by using devices such as the Motorola Network Encryption System (NES) to tunnel the unclassified data across the SECRET internet. In general it is expected that the smaller and more mobile a unit is, the fewer unclassified users the unit will have. Therefore, most of the unclassified IP addresses are allocated to large units and/or units whose mission is primarily combat service support (CSS).

Each Tactical Data Network Gateway is assigned both a classified and unclassified class C network number. Each TDN Gateway has two complete suites of equipment that can support two physically separate IP networks. TDN Gateways are expected to be the major data networking hubs in the Marine Corps tactical internet. However the concept of employment for the TDN Gateway is not yet well-defined and it is uncertain exactly what its IP address requirements will be. Therefore sufficient IP address space is allocated to each of the Gateways to ensure maximum employment flexibility.

C. COMMAND ELEMENT

1. Marine Component HQ

The actual structure, employment and support of a Marine component command headquarters in the field has not been well established in doctrine. This is an area that is the subject of much development effort within the Marine Corps. Therefore, two class C network numbers (512 IP host addresses) are assigned to each MARFOR headquarters but no internal address assignment is shown.

2. Marine Expeditionary Units (MEUs)

Four class C addresses were assigned to each MEU. A MEU consists of a command element, an infantry battalion landing team, an aircraft squadron and a combat

service support unit. Due the unpredictable nature of MEU operations and the discontinuous topology of MEU networks, four class C network addresses (one for each element) were assigned to each MEU. However, the internal breakdown of the MEU's address assignment is not shown.

3. Contingency Joint Task Force (JTF)

Each MEF is required to maintain a contingency capability to deploy as a nucleus Joint Task Force Headquarters. The IP address requirements for this nucleus JTF are unknown but two class C addresses is consistent with that of the MARFOR headquarters. Further, additional IP addresses can be provided from the MEF's contingency address block if necessary.

4. Marine Expeditionary Force Command Element

a. MEF Main Command Post (CP)

In a large scale expeditionary operation, the MEF is the principal warfighting entity of the Marine Corps. The MEF main command post is also the principal networking hub for FMF units in the area of operations. The MEF TDN Gateway will serve as the Marine Corps' connection to the joint internet, interconnecting the Division, Wing, and FSSG TDN Gateways. The proposed standard address assignment for the MEF TDN Gateway is shown in Table A.3. The IP address space for the Gateway is partitioned into variable length subnets for maximum use of the class C address. The first subnet generally follows the generic template example shown in Chapter VII. Subnets *N.N.16.160* and *N.N.16.176* are for use in connecting the TDN Servers in the MEF command post to the Gateway and to each other. The remainder of the class C address is partitioned into 4-bit subnets that can be used on serial communications links between routers, with the last four reserved for dial-in access. The other class C network assigned to the MEF command post is for use in the MEF combat operations center (COC) and the

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
MEF TDN GW	N.N.16.0	N.N.16.0	N.N.16.1-6	router
		(3 bit subnet)	N.N.16.7	DMS IMTA
			N.N.16.8	SNS/NES/INE
			N.N.16.9	DNS server
			N.N.16.10	DHCP server
			N.N.16.11	SMTP mail server
			N.N.16.12-13	management workstations
			N.N.16.14-17	UPSs and printers
			N.N.16.18-21	Ext Drives/RAID
			N.N.16.22-26	TCIMs
			N.N.16.27-30	repeaters
			N.N.16.31	subnet broadcast
	3 bit subnets->	N.N.16.32	N.N.16.33-62	users/ devices
		N.N.16.64	N.N.16.65-95	users/ devices
		N.N.16.96	N.N.16.97-126	users/ devices
		N.N.16.128	N.N.16.129-158	users/ devices
	start 4 bit subnets->	N.N.16.160	N.N.16.161-174	Server subnet
		N.N.16.176	N.N.16.177-190	Server subnet
	start 6 bit subnets->	N.N.16.192	N.N.16.193-194	16 serial line
		N.N.16.196	N.N.16.197-198	PPP subnets
		N.N.16.200	N.N.16.201-202	with 2 endpts
		N.N.16.204	N.N.16.205-206	per subnet
		N.N.16.208	N.N.16.209-210	
		N.N.16.212	N.N.16.213-214	
		N.N.16.216	N.N.16.217-218	
		N.N.16.220	N.N.16.221-222	
		N.N.16.224	N.N.16.225-226	
		N.N.16.228	N.N.16.229-230	
		N.N.16.232	N.N.16.233-234	
		N.N.16.236	N.N.16.237-238	
		N.N.16.240	N.N.16.241-242	Dial up PPP subnet
		N.N.16.244	N.N.16.245-246	Dial up PPP subnet
		N.N.16.248	N.N.16.249-250	Dial up PPP subnet
		N.N.16.252	N.N.16.253-254	Dial up PPP subnet

Table A.3 Example IP address assignment for the MEF TDN Gateway.

MEF staff section areas (G sections). It is anticipated that the MEF CP will utilize two TDN Servers to connect all of its LAN users.

Therefore the MEF main CP class C address is partitioned into two subnets of 128 host addresses each as shown in Table A.4. The assignment within the subnets follows the generic TDN LAN addressing template. If the MEF employs a Forward CP, it would be addressed in accordance with Table A.8. Eight (8) additional class C addresses have been reserved for the MEF's use in case of contingencies.

b. Communications Battalion

The Communications Battalion provides the communications and networking support for the MEF Command Element. The Battalion will almost always colocate with the MEF main command post and will establish its own internal local-area network. The Communication Battalion IP address assignment is shown in Table A.5. Although the assignment follows the generic template, note that two class C network numbers are reserved for IP addressing of communications equipment.

c. Surveillance, Reconnaissance, and Intelligence Group (SRIG) Headquarters and Radio Battalion

SRIG is a subordinate unit of the MEF Command Element. The SRIG is composed of the Communications Battalion, the Radio Battalion, and a number of smaller units that utilize remote sensors (UAVs and ground sensors). Therefore, the SRIG's IP network number was partitioned as shown in Table A.6 to allow sufficient address for these remote sensors to given IP addresses.

The Radio Battalion is concerned mainly with signals intelligence and electronic warfare. This battalion will typically establish a command center in close proximity to the SRIG/MEF command post. Radio Battalion contains many items of communications-electronic equipment which may ultimately be networked. Therefore Radio Battalion is allocated sufficient addresses (Table A.7) to establish its own LAN and permit IP addressing of its many communication-electronic devices.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
MEF COC	N.N.17.0	N.N.17.0	N.N.17.1-5	router
		(1 bit subnet)	N.N.17.6	LAN file server
			N.N.17.7	DMS MTA
			N.N.17.8	SNS/NES/INE
			N.N.17.9	DNS server
			N.N.17.10	DHCP server
			N.N.17.11	SMTP mail server
			N.N.17.12	Web server
			N.N.17.13	management workstation
			N.N.17.14-16	UPSs
			N.N.17.17-20	External drives/RAID
			N.N.17.21-24	TCIMs
			N.N.17.25-30	repeaters
			N.N.17.31-33	reserved
			N.N.17.34	main TCO workstation
			N.N.17.35-126	MEF COC users
			N.N.17.127	subnet broadcast
MEF G sections	N.N.17.0	N.N.17.128	N.N.17.129-133	router addresses
		(1 bit subnet)	N.N.17.134	LAN file server
			N.N.17.135	DMS MTA
			N.N.17.136	SNS/NES/INE
			N.N.17.137	DNS server
			N.N.17.138	DHCP server
			N.N.17.139	SMTP mail server
			N.N.17.140	Web server
			N.N.17.141	management workstation
			N.N.17.142-144	UPSs
			N.N.17.145-148	External drives/RAID
			N.N.17.149-152	TCIMs
			N.N.17.153-158	repeaters
			N.N.17.159-254	MEF G section users
			N.N.17.255	subnet broadcast

Table A.4 Example IP address allocation for the MEF Main Command Post.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Communications Bn	N.N.18.0	None	N.N.18.1-5	router
			N.N.18.6	LAN file server
			N.N.18.7	DMS MTA
			N.N.18.8	SNS/NES/INE
			N.N.18.9	DNS server
			N.N.18.10	DHCP server
			N.N.18.11	SMTP mail server
			N.N.18.12	Web server
			N.N.18.13	management workstation
			N.N.18.14-16	UPSs/external drives/RAID
			N.N.18.17-20	External drives/RAID
			N.N.18.21-24	TCIMs
			N.N.18.25-30	repeaters
			N.N.18.31-33	reserved
			N.N.18.34	main TCO workstation
			N.N.18.35-254	Comm Bn users
			N.N.18.255	subnet broadcast
Communications Bn	N.N.19.0	None	N.N.19.1-254	reserved for future IP addressing of comm equipment
Communications Bn	N.N.20.0	None	N.N.20.1-254	reserved for future IP addressing of comm equipment

Table A.5 Example IP address plan for Communications Battalion.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
SRIG Headquarters	N.N.21.0	N.N.21.0	N.N.21.1-5	router
		(1 bit subnet)	N.N.21.6	LAN file server
			N.N.21.7	DMS MTA
			N.N.21.8	SNS/NES/INE
			N.N.21.9	DNS server
			N.N.21.10	DHCP server
			N.N.21.11	SMTP mail server
			N.N.21.12	Web server
			N.N.21.13	management workstation
			N.N.21.14-16	UPSs
			N.N.21.17-20	External drives/RAID
			N.N.21.21-24	TCIMs
			N.N.21.25-30	repeaters
			N.N.18.31-33	reserved
			N.N.21.34	main TCO workstation
			N.N.21.35-126	SRIG HQ users
			N.N.21.2127	subnet broadcast
SRIG Sensing Units	N.N.21.0	N.N.21.128 (1bit subnet)	N.N.21.129-254	reserved for IP addressing of remote sensing equipment

Table A.6 Example IP address plan for the Surveillance, Reconnaissance, and Intelligence Group.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Radio Battalion	N.N.22.0	None	N.N.22.1-5	router
			N.N.22.6	LAN file server
			N.N.22.7	DMS MTA
			N.N.22.8	SNS/NES/INE
			N.N.22.9	DNS server
			N.N.22.10	DHCP server
			N.N.22.11	SMTP mail server
			N.N.22.12	Web server
			N.N.22.13	management workstation
			N.N.22.14-16	UPSs
			N.N.22.17-20	External drives/RAID
			N.N.22.21-24	TCIMs
			N.N.22.25-30	repeaters
			N.N.22.31-33	reserved
			N.N.22.34	main TCO workstation
			N.N.22.35-126	Radio Bn users
			N.N.22.127	subnet broadcast
Radio Battalion			N.N.22.129-254	reserved for IP addressing of electronic sensing equipment

Table A.7 Example IP address plan for Radio Battalion.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
MEF Forward Command Post	N.N.23.0	None	N.N.23.1-5	router
			N.N.23.6	LAN file server
			N.N.23.7	DMS MTA
			N.N.23.8	SNS/NES/INE
			N.N.23.9	DNS server
			N.N.23.10	DHCP server
			N.N.23.11	SMTP mail server
			N.N.23.12	Web server
			N.N.23.13	management workstation
			N.N.23.14-16	UPSs
			N.N.23.17-20	External drives/RAID
			N.N.23.21-24	TCIMs
			N.N.23.25-30	repeaters
			N.N.23.31-33	reserved
			N.N.23.34	main TCO workstation
			N.N.23.35-254	MEF FWD CP users
			N.N.23.255	subnet broadcast

Table A.8 Example IP address plan for MEF Forward Command Post.

D. GROUND COMBAT ELEMENT (GCE)

1. Marine Division Main Command Post (CP)

The Division Main CP is the internetworking hub for the entire ground combat element in a large scale operation. The IP address assignment table for the Division's TDN Gateway is shown in Table A.9. The assignment patterns for all TDN Gateways is identical. The IP address assignments for the Division Main Combat Operations Center (COC) and Division staff sections is shown in Table A.10. This assignment is very similar to the MEF CP address allocation table. It is expected that the Division will employ two TDN servers in the Division Main command post, one for classified and one for unclassified. Therefore each of the Division Main class C network numbers (one classified and one unclassified) is partitioned between the COC and the staff sections.

2. Division Forward and Rear Command Posts

It is uncertain whether the Division Forward CP will employ a TDN Server LAN or not. If so, IP addresses would be assignment in the same manner shown for the MEF Forward CP in Table A.8. The Division Rear CP may employ two TDN LANs, one for classified and one for unclassified. Therefore the Division Rear CP is provided its own class C network addresses.

3. Direct Air Support Center (DASC)

The DASC will typically locate with the Division Fire Support Coordination Center (FSCC) in the Division Main CP. For this reason, the DASC is assigned a network number out of the GCE address block and not out of the ACE block. Because the DASC can also locate with infantry regiments on smaller operations, it was provided its own network number instead of a subnet number from the Division CP.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Division TDN GW	N.N.32.0	N.N.32.0	N.N.32.1-6	router
		(3 bit subnet)	N.N.32.7	DMS IMTA
			N.N.32.8	SNS/NES/INE
			N.N.32.9	DNS server
			N.N.32.10	DHCP server
			N.N.32.11	SMTP mail server
			N.N.32.12-13	management workstations
			N.N.32.14-17	UPSs and printers
			N.N.32.18-21	Ext Drives/RAID
			N.N.32.22-26	TCIMs
			N.N.32.27-30	repeaters
			N.N.32.31	subnet broadcast
	3 bit subnets->	N.N.32.32	N.N.32.33-62	LAN users/ devices
		N.N.32.64	N.N.32.65-95	LAN users/ devices
		N.N.32.96	N.N.32.97-126	LAN users/ devices
		N.N.32.128	N.N.32.129-158	LAN users/ devices
Division TDN GW	start 4 bit subnets->	N.N.32.160	N.N.32.161-174	Server-server subnet
		N.N.32.176	N.N.32.177-190	Server-server subnet
	start 6 bit subnets->	N.N.32.192	N.N.32.193-194	16 serial line
		N.N.32.196	N.N.32.197-198	PPP subnets
		N.N.32.200	N.N.32.201-202	with 2 endpts
		N.N.32.204	N.N.32.205-206	per subnet
		N.N.32.208	N.N.32.209-210	
		N.N.32.212	N.N.32.213-214	
		N.N.32.216	N.N.32.217-218	
		N.N.32.220	N.N.32.221-222	
		N.N.32.224	N.N.32.225-226	
		N.N.32.228	N.N.32.229-230	
		N.N.32.232	N.N.32.233-234	
		N.N.32.236	N.N.32.237-238	
		N.N.32.240	N.N.32.241-242	Dial up PPP subnet
		N.N.32.244	N.N.32.245-246	Dial up PPP subnet
		N.N.32.248	N.N.32.249-250	Dial up PPP subnet
		N.N.32.252	N.N.32.253-254	Dial up PPP subnet

Table A.9 Example IP address plan for the Marine Division TDN Gateway.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Division COC	N.N.33.0	N.N.33.0	N.N.33.1-5	router
		(1 bit subnet)	N.N.33.6	LAN file server
			N.N.33.7	DMS MTA
			N.N.33.8	SNS/NES/INE
			N.N.33.9	DNS server
			N.N.33.10	DHCP server
			N.N.33.11	SMTP mail server
			N.N.33.12	Web server
			N.N.33.13	management workstation
			N.N.33.14-16	UPSs
			N.N.33.17-20	External drives/RAID
			N.N.33.21-24	TCIMs
			N.N.33.25-30	repeaters
			N.N.33.31-33	reserved
			N.N.33.34	main TCO workstation
			N.N.33.35-126	DIV COC users
			N.N.33.127	subnet broadcast
Division G sections	N.N.33.0	N.N.33.128	N.N.33.129-133	router addresses
		(1 bit subnet)	N.N.33.134	LAN file server
			N.N.33.135	DMS MTA
			N.N.33.136	SNS/NES/INE
			N.N.33.137	DNS server
			N.N.33.138	DHCP server
			N.N.33.139	SMTP mail server
			N.N.33.140	Web server
			N.N.33.141	management workstation
			N.N.33.142-144	UPSs
			N.N.33.145-148	External drives/RAID
			N.N.33.149-152	TCIMs
			N.N.33.153-158	repeaters
			N.N.33.159-254	Division G section users
			N.N.33.255	subnet broadcast

Table A.10 Example IP address plan for the Marine Division Main Command Post.

4. Combat Engineer Battalion (CEB)

The Combat Engineer Battalion (CEB) is a separate battalion under the direct command of the Marine Division. In practice CEB often establishes its battalion command post near the Division main CP. Nonetheless CEB is an independent unit with its own TDN network and is assigned its own SECRET class C network number. CEB shares an unclassified network address with the DASC. Internal IP address assignment is according to the generic template.

5. Artillery Regiment

There is one Artillery Regiment in the Division. The Headquarters Battery of the Artillery Regiment is quite large with a wide variety of support personnel. The regimental main command post consists of a Fire Direction Center (FDC) that will support at least eight AFATDS terminals in addition to two TCO terminals and other tactical data systems. The regiment also maintains a large maintenance capability that may be located in the main CP or in a logistics support area (LSA). It is expected that an artillery regiment will establish two or three TDN LANs, therefore three class C network numbers are allocated. The FDC address is partitioned into user subnets and serial line subnets that are used to connect the artillery battalions to the regiment. It is expected that most of the traffic at the Artillery Regiment and below will be classified, and that at most one unclassifed TDN Server will be employed. Therefore two unclassified network addresses are allocated to cover the regiment and its artillery battalions.

6. Artillery Battalions

Artillery battalions are data-intensive organizations. As the digitization of fire support continues, the artillery must be fully internetworked down to the gun line. Each artillery battalion will receive one TDN Server which will certainly be employed at the battalions' main CPs. However there is a need to assign IP addresses to all fire support devices and AFATDS terminals in the battalion. Therefore a class C network number

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Artillery Regiment	N.N.40.0	N.N.40.0	N.N.40.1-5	router
Main Command Post		(2 bit subnet)	N.N.40.6	LAN file server
			N.N.40.7	DMS MTA
			N.N.40.8	SNS/NES/INE
			N.N.40.9	DNS server
			N.N.40.10	DHCP server
			N.N.40.11	SMTP mail server
			N.N.40.12	Web server
			N.N.40.13-14	management workstations
			N.N.40.15-17	UPSs
			N.N.40.18-21	External drives/RAID
			N.N.40.22-25	TCIMs
			N.N.40.26-30	repeaters
			N.N.40.31-33	reserved
			N.N.40.34	main TCO workstation
			N.N.40.34-62	Regtimental FDC LAN users/ devices
	2 bit subnets->	N.N.40.64	N.N.40.65-126	Regt FDC users/devices
		N.N.40.128	N.N.40.129-190	Regt FDC users/devices
Arty Main CP Server	start 6 bit subnets->	N.N.40.192	N.N.40.193-194	16 serial line
		N.N.40.196	N.N.40.197-198	PPP subnets
		N.N.40.200	N.N.40.201-202	with 2 endpts
		N.N.40.204	N.N.40.205-206	per subnet
		N.N.40.208	N.N.40.209-210	
		N.N.40.212	N.N.40.213-214	
		N.N.40.216	N.N.40.217-218	
		N.N.40.220	N.N.40.221-222	
		N.N.40.224	N.N.40.225-226	
		N.N.40.228	N.N.40.229-230	
		N.N.40.232	N.N.40.233-234	
		N.N.40.236	N.N.40.237-238	
		N.N.40.240	N.N.40.241-242	
		N.N.40.244	N.N.40.245-246	
		N.N.40.248	N.N.40.249-250	
		N.N.40.252	N.N.40.253-254	
Arty Logistics Support	N.N.41.0		N.N.41.1-254	Arty LSA LAN
Arty Regt FWD CP	N.N.42.0		N.N.42.1-254	Arty FWD CP LAN

Table A.11 Example IP address plan for an Artillery Regiment.

was allocated to each artillery battalion and partitioned to give each battery a group of subnet addresses. A sample artillery battalion allocation is shown in Table A.12.

7. Infantry Regiments

There are usually three infantry regiments in the Marine Divison. Each regiment will receive three TDN Servers. The infantry regiment typically installs a LAN only at its main command post because its forward CP is highly mobile. Infantry regimental headquarters are not large enough to support rear CPs. Therefore each infantry regiment was allocated one classified network address and two unclassified addresses which must be shared among itself and its three infantry battalions. As shown in Table A.13, the partitioning of the infantry regiment's class C network address as similar to that of the artillery regiment's FDC address.

8. Infantry Battalions

There are three infantry battalions in each regiment. Each battalion has three rifle companies and one weapons company. One TDN Server will be fielded to each infantry battalion. Since a battalion can operate independently, each battalion was assigned a separate network number. The proposed IP address assignment shown in Table A.14 is identical to the generic template. Currently infantry battalions only occasionally set up LANs, but this will not be the case in the future. Advances in radio-based networking will allow battalions to remain fully internetworked with the MEF at all times. Further, the infantry battalion is likely to see a proliferation of handheld data communications devices which must all be assigned IP addresses. Therefore a class C network number is needed to ensure sufficient address space to accommodate these changes.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
1st Artillery Battalion	N.N.43.0	N.N.43.0	N.N.43.1-5	router
Main Command Post		(1 bit subnet)	N.N.43.6	LAN file server
			N.N.43.7	DMS MTA
			N.N.43.8	SNS/NES/INE
			N.N.43.9	DNS server
			N.N.43.10	DHCP server
			N.N.43.11	SMTP mail server
			N.N.43.12	Web server
			N.N.43.13	management workstation
			N.N.43.14-16	UPSs
			N.N.43.17-20	External drives/RAID
			N.N.43.21-24	TCIMs
			N.N.43.25-30	repeaters
			N.N.43.31-33	reserved
			N.N.43.34	mainTCO workstation
			N.N.43.35-126	Battalion FDC LAN users/ devices
Artillery Batteries	3 bit subnets start->	N.N.43.128	N.N.43.129-158	A Battery LAN
		N.N.43.160	N.N.43.161-190	B Battery LAN
		N.N.43.192	N.N.43.193-222	C Battery LAN
		N.N.43.224	N.N.43.225-254	Spare

Table A.12 Example IP address plan for an Artillery Battalion.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
1st Infantry Regiment	N.N.48.0	N.N.48.0	N.N.48.1-5	router
Main Command Post		(2 bit subnet)	N.N.48.6	LAN file server
			N.N.48.7	DMS MTA
			N.N.48.8	SNS/NES/INE
			N.N.48.9	DNS server
			N.N.48.10	DHCP server
			N.N.48.11	SMTP mail server
			N.N.48.12	Web server
			N.N.48.13-14	management workstations
			N.N.48.15-17	UPSs
			N.N.48.18-21	External drives/RAID
			N.N.48.22-25	TCIMs
			N.N.48.26-30	repeaters
			N.N.48.31-33	reserved
			N.N.48.34	main TCO workstation
			N.N.48.35-62	Regt LAN users
	2 bit subnet->	N.N.48.64	N.N.48.65-126	Regt LAN users
	2 bit subnet->	N.N.48.128	N.N.48.129-190	Regt LAN users
	start 6 bit subnets->	N.N.48.192	N.N.48.193-194	16 serial line
		N.N.48.196	N.N.48.197-198	PPP subnets
		N.N.48.200	N.N.48.201-202	with 2 endpts
		N.N.48.204	N.N.48.205-206	per subnet
		N.N.48.208	N.N.48.209-210	
		N.N.48.212	N.N.48.213-214	
		N.N.48.216	N.N.48.217-218	
		N.N.48.220	N.N.48.221-222	
		N.N.48.224	N.N.48.225-226	
		N.N.48.228	N.N.48.229-230	
		N.N.48.232	N.N.48.233-234	
		N.N.48.236	N.N.48.237-238	
		N.N.48.240	N.N.48.241-242	
		N.N.48.244	N.N.48.245-246	
		N.N.48.248	N.N.48.249-250	
		N.N.48.252	N.N.48.253-254	

Table A.13 Example IP address plan for an Infantry Regiment.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
1st Infantry Bn, 1st Infantry Regiment	N.N.49.0	None	N.N.49.1-5	router
			N.N.49.6	LAN file server
			N.N.49.7	DMS MTA
			N.N.49.8	SNS/NES/INE
			N.N.49.9	DNS server
			N.N.49.10	DHCP server
			N.N.49.11	SMTP mail server
			N.N.49.12	Web server
			N.N.49.13	management workstation
			N.N.49.14-16	UPSs
			N.N.49.17-20	External drives/RAID
			N.N.49.21-24	TCIMs
			N.N.49.25-30	repeaters
			N.N.49.31-33	reserved
			N.N.49.34	main TCO workstation
			N.N.49.35-254	Inf Bn and Inf Company users
			N.N.49.255	subnet broadcast

Table A.14 Example IP address plan for an Infantry Battalion.

9. Tank Battalion/Light Armored Reconnaissance Battalion

These two battalions are similar in the structure of their networks. Each unit can either operate as a whole or can detach its companies to support other units. Since the armored vehicles will certainly have addressable devices in them, separate subnets were assigned to each company in addition to the subnet for the battalion LAN. This breakdown is shown in Tables A.15 and A.16.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Tank Battalion	N.N.60.0	N.N.60.0	N.N.60.1-5	router
Main Command Post			N.N.60.6	LAN file server
			N.N.60.7	DMS MTA
			N.N.60.8	SNS/NES/INE
			N.N.60.9	DNS server
			N.N.60.10	DHCP server
			N.N.60.11	SMTP mail server
			N.N.60.12	Web server
			N.N.60.13	management workstation
			N.N.60.14-16	UPSs
			N.N.60.17-20	External drives/RAID
			N.N.60.21-24	TCIMs
			N.N.60.25-30	repeaters
			N.N.60.31	subnet broadcast
	3 bit subnet->	N.N.60.32	N.N.60.34	main TCO workstation
			N.N.60.35-62	Tank Bn LAN users
	3 bit subnets->	N.N.60.64	N.N.60.65-95	Tank Bn LAN users
Anti-Tank Company		N.N.60.96	N.N.60.97-126	Anti-Tank Company
Tank Companies		N.N.60.128	N.N.60.129-158	Tank Company
		N.N.60.160	N.N.60.161-190	Tank Company
		N.N.60.192	N.N.60.193-222	Tank Company
		N.N.60.224	N.N.60.225-254	Tank Company

Table A.15 Example IP address plan for Tank Battalion.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
LAV/LAR Battalion	N.N.61.0	N.N.61.0	N.N.61.1-6	router
Main Command Post			N.N.61.6	LAN file server
			N.N.61.7	DMS MTA
			N.N.61.8	SNS/NES/INE
			N.N.61.9	DNS server
			N.N.61.10	DHCP server
			N.N.61.11	SMTP mail server
			N.N.61.12	Web server
			N.N.61.13	management workstation
			N.N.61.14-16	UPSs
			N.N.61.17-20	External drives/RAID
			N.N.61.21-24	TCIMs
			N.N.61.25-30	repeaters
			N.N.61.31	subnet broadcast
	3 bit subnet->	N.N.61.32	N.N.61.34	main TCO workstation
			N.N.61.35-62	LAR Bn LAN users
	3 bit subnets->	N.N.61.64	N.N.61.65-95	LAR Bn LAN users
LAV/LAR Companies		N.N.61.96	N.N.61.97-126	LAV/LAR Company
		N.N.61.128	N.N.61.129-158	LAV/LAR Company
		N.N.61.160	N.N.61.161-190	LAV/LAR Company
		N.N.61.192	N.N.61.193-222	LAV/LAR Company
		N.N.61.224	N.N.61.225-254	LAV/LAR Company

Table A.16 Example IP address plan for Light Armored Reconnaissance Battalion.

10. Assault Amphibian Battalion

The Assault Amphibian Battalion is the largest battalion in the Division. The battalion contains nearly 200 amphibious assault vehicles (AAVs) each of which has numerous radio and electronic equipment on board. In addition to the battalion headquarters LAN IP address requirements, there will be a need to assign at least one IP address to every AAV. Further, the AAV command and control variant (AAVC-7) will require an entire subnet itself. Given the current equipment suite in the AAVC-7, and that projected for the follow-on AAAV, 16 addresses per vehicle should be sufficient. The allocation of the two class C network numbers assigned to the AA Battalion is shown in Table A.17.

E. AVIATION COMBAT ELEMENT (ACE)

1. Marine Air Wing Headquarters/Tactical Air Command Center (TACC)

The TACC is the command and control hub for Marine aviation in the area of operations. Therefore, the TACC is accompanied by the major networking equipment of the Air Wing. It is expected that the Wing TDN Gateway will be located in the same command post with the TACC and the Wing headquarters staff. The address allocation for the Wing TDN Gateway shown in Table A.18 is identical that of the MEF Gateway. The TACC will have its own TDN Server to network its many tactical data systems. Table A.19 shows the notional assignment of TACC IP addresses. In addition to the subnets provided for general TACC LAN users, separate subnets (64 IP addresses per subnet) are allocated for both the Advance Tactical Air Command Center (ATACC) and the Contingency Theater Air Planning System (CTAPS). The ATACC system currently consists of 10 end systems and the TACC employs approximately 20 CTAPS terminals. It is anticipated that most of the TACC data traffic will be SECRET, so the TACC and the Wing headquarters will share a class C unclassified network number.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
AAV Battalion	N.N.62.0	N.N.62.0	N.N.62.1-5	router
Main Command Post			N.N.62.6	LAN file server
			N.N.62.7	DMS MTA
			N.N.62.8	SNS/NES/INE
			N.N.62.9	DNS server
			N.N.62.10	DHCP server
			N.N.62.11	SMTP mail server
			N.N.62.12	Web server
			N.N.62.13	management workstation
			N.N.62.14-16	UPSs
			N.N.62.17-20	External drives/RAID
			N.N.62.21-24	TCIMs
			N.N.62.25-30	repeaters
			N.N.62.31-33	reserved
			N.N.62.34	main TCO workstation
			N.N.62.35-126	AAV Bn LAN users
	4 bit subnets->	N.N.62.128	N.N.62.129-130	AAVC7
		N.N.62.144	N.N.62.145-146	AAVC7
		N.N.62.160	N.N.62.161-174	AAVC7
		N.N.62.176	N.N.62.177-190	AAVC7
		N.N.62.192	N.N.62.193-206	AAVC7
		N.N.62.208	N.N.62.209-222	AAVC7
		N.N.62.224	N.N.62.225-238	AAVC7
		N.N.62.240	N.N.62.241-254	AAVC7
AAV Line Companies	N.N.63.0	N.N.63.0	N.N.63.1-62	A Co AAV Bn
	2 bit subnets->	N.N.63.64	N.N.63.65-126	B Co AAV Bn
		N.N.63.128	N.N.63.129-190	C Co AAV Bn
		N.N.63.192	N.N.63.193-254	D Co AAV Bn

Table A.17 Example IP address plan for Assault Amphibian Battalion.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Marine Air Wing TDN GW	N.N.64.0	N.N.64.0	N.N.64.1-6	router
			N.N.64.7	DMS IMTA
			N.N.64.8	SNS/NES/INE
			N.N.64.9	DNS server
			N.N.64.10	DHCP server
			N.N.64.11	SMTP mail server
			N.N.64.12-13	management workstations
			N.N.64.14-17	UPSs and printers
			N.N.64.18-21	External drives/RAID
			N.N.64.22-26	TCIMs
			N.N.64.27-30	repeaters
			N.N.64.31	subnet broadcast
	3 bit subnets->	N.N.64.32	N.N.64.33-62	LAN users/ devices
		N.N.64.64	N.N.64.65-95	LAN users/ devices
		N.N.64.96	N.N.64.97-126	LAN users/ devices
		N.N.64.128	N.N.64.129-158	LAN users/ devices
MAW TDN GW	start 4 bit subnets->	N.N.64.160	N.N.64.161-174	Server-server subnet
		N.N.64.176	N.N.64.177-190	Server-server subnet
	start 6 bit subnets->	N.N.64.192	N.N.64.193-194	16 serial line
		N.N.64.196	N.N.64.197-198	PPP subnets
		N.N.64.200	N.N.64.201-202	with 2 endpts
		N.N.64.204	N.N.64.205-206	per subnet
		N.N.64.208	N.N.64.209-210	
		N.N.64.212	N.N.64.213-214	
		N.N.64.216	N.N.64.217-218	
		N.N.64.220	N.N.64.221-222	
		N.N.64.224	N.N.64.225-226	
		N.N.64.228	N.N.64.229-230	
		N.N.64.232	N.N.64.233-234	
		N.N.64.236	N.N.64.237-238	
		N.N.64.240	N.N.64.241-242	Dial up PPP subnet
		N.N.64.244	N.N.64.245-246	Dial up PPP subnet
		N.N.64.248	N.N.64.249-250	Dial up PPP subnet
		N.N.64.252	N.N.64.253-254	Dial up PPP subnet

Table A.18 Example IP address plan for the Marine Air Wing TDN Gateway.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Tactical Air Command Center (TACC)	N.N.65.0	N.N.65.0	N.N.65.1-5	router
			N.N.65.6	LAN file server
			N.N.65.7	DMS MTA
			N.N.65.8	SNS/NES/INE
			N.N.65.9	DNS server
			N.N.65.10	DHCP server
			N.N.65.11	SMTP mail server
			N.N.65.12	Web server
			N.N.65.13	management workstation
			N.N.65.14-16	UPSs
			N.N.65.17-20	External drives/RAID
			N.N.65.21-24	TCIMs
			N.N.65.25-30	repeaters
			N.N.65.31-33	reserved
			N.N.65.34	main TCO workstation
			N.N.65.35-62	TACC LAN users
	2 bit subnets->	N.N.65.64	N.N.65.66-126	ATACC
		N.N.65.128	N.N.65.129-190	CTAPS
		N.N.65.192	N.N.65.193-222	TACC LAN users
		N.N.65.224	N.N.65.225-254	TACC LAN users

Table A.19 Example IP address plan for the Tactical Air Command Center.

The Wing headquarters and staff sections will have their own LAN using a separate TDN Server. Therefore a separate class C address is provided for Wing headquarters. The IP address assignment for the Wing HQ is shown in Table A.20.

2. Marine Wing Support Group (MWSG) and Marine Air Control Group(MACG)

These two elements of the Marine Air Wing typically colocate with the TACC and Wing HQ. However, each will have its own TDN Servers and many LAN users. Therefore each of these units was allocated both a classified and unclassified class C network. Internal allocations of addresses are in accordance with the basic template and therefore are not shown in a separate table.

3. Marine Wing Communications Squadron

The communications squadron provides the communications interconnectivity for the TACC, the Wing HQ and most of the Marine Air Wing's subordinate units. The communications squadron headquarters area is in the command post with the TACC and Wing HQ. The squadron will have its own LANs and TDN servers, so it is provided separate class C network numbers. The assignment of these addresses is shown in Table A. 21. Like the communications battalion, the communications squadron may need IP addresses to assign to it communications equipment in the future.

4. Fixed/Rotary Wing Marine Air Groups (MAGs)

There are two fixed wing MAGs and two rotary wing MAGs in the Marine Air Wing. Each MAG is an independent unit and will have its own network, therefore each is assigned its own class C network number. The partitioning of the MAG's class C address is shown in Table A.22. Note that a MAG will be located at an airfield. Therefore, a subnet is dedicated to connecting all of the squadron LANs together, and two subnets are provided to the Marine Air Traffic Control Squadron detachment at the airfield.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Marine Wing Command Element	N.N.66.0	None	N.N.66.1-5	router
			N.N.66.6	LAN file server
			N.N.66.7	DMS MTA
			N.N.66.8	SNS/NES/INE
			N.N.66.9	DNS server
			N.N.66.10	DHCP server
			N.N.66.11	SMTP mail server
			N.N.66.12	Web server
			N.N.66.13	management workstation
			N.N.66.14-16	UPSs
			N.N.66.17-20	External drives/RAID
			N.N.66.21-24	TCIMs
			N.N.66.25-30	repeaters
			N.N.66.31-33	reserved
			N.N.66.34	main TCO workstation
			N.N.66.35-254	Wing staff sections LAN users
			N.N.66.255	network broadcast

Table A.20 Example IP address plan for Marine Air Wing Command Element

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Marine Wing Communication Sqdn	N.N.69.0	N.N.69.0 (1 bit subnet)	N.N.69.1-5	router
			N.N.69.6	LAN file server
			N.N.69.7	DMS MTA
			N.N.69.8	SNS/NES/INE
			N.N.69.9	DNS server
			N.N.69.10	DHCP server
			N.N.69.11	SMTP mail server
			N.N.69.12	Web server
			N.N.69.13	management workstation
			N.N.69.14-16	UPSs
			N.N.69.17-20	External drives/RAID
			N.N.69.21-24	TCIMs
			N.N.69.25-30	repeaters
			N.N.69.31-33	reserved
			N.N.69.34	main TCO workstation
			N.N.69.35-126	Comm SQDN LAN users
			N.N.69.127	subnet broadcast
Communication Squadron		N.N.69.128 (1 bit subnet)	N.N.69.129-254	reserved for IP addressing of communications equipment

Table A.21 Example IP address plan for Marine Wing Communications Squadron.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
Fixed Wing MAG	N.N.72.0	N.N.72.0	N.N.72.1-5	router
		(1 bit subnet)	N.N.72.6	LAN file server
			N.N.72.7	DMS MTA
			N.N.72.8	SNS/NES/INE
			N.N.72.9	DNS server
			N.N.72.10	DHCP server
			N.N.72.11	SMTP mail server
			N.N.72.12	Web server
			N.N.72.13	management workstation
			N.N.72.14-16	UPSs
			N.N.72.17-20	External drives/RAID
			N.N.72.21-24	TCIMs
			N.N.72.25-30	repeaters
			N.N.72.31-33	reserved
			N.N.72.34	main TCO workstation
			N.N.72.35-126	MAG HQ LAN users
			N.N.72.127	subnet broadcast
	3 bit subnets->	N.N.72.128	N.N.72.129-158	Airfield server to server LAN
MATCS		N.N.72.160	N.N.72.161-190	reserved for router and server functions
		N.N.72.192	N.N.72.193-222	MATCS LAN users
		N.N.72.224	N.N.72.225-254	MATCS LAN users

Table A.22 Example IP address plan for a Fixed Wing Marine Air Group and Marine Air Traffic Control Squadron.

5. Marine Aviation Logistics Squadron (MALS) and Marine Wing Support Squadron (MWSS)

Each MAG has both a MALS and an MWSS. These units provide maintenance, engineering and overall combat service support to the MAG and its squadrons. MALS and MWSS will typically colocate with the MAG headquarters at an airfield. Since they are independent units with a potentially large number of LAN users, each was given its own class C network address. The internal address assignment is accordance with the basic template.

6. Fixed/Rotary Wing Squadrons

Although there are more fixed wing than rotary wing squadrons, networks of the two squadron types will be quite similar. Each squadron, like each infantry battalion, is capable of independent employment and each receives its own class C network number. The assignment of squadron IP addresses is just like that of the infantry battalion shown in Table A.14.

7. Marine Air Control Squadron (MACS)

There are two MACS in each Marine Air Wing. The mission of the MACS is to set up the Tactical Air Operations Center (TAOC) which is the center for air defense in the Marine area of operations. Doctrinally, two TAOCs might be set up in the same area of operations, so each squadron was allocated its own class C network number. The IP address assignment within the MACS LAN is according to the basic template. The TAOC contains many communications and information systems devices that may eventually need to be given IP addresses.

8. Low Altitude Air Defense (LAAD) Battalion

The LAAD battalion is similar in structure to an artillery battalion. There is a headquarters element and several LAAD batteries. Since LAAD is an independent unit it is assigned a separate class C network number. Table A.23 shows the partitioning of the

LAAD network address. The LAAD batteries have tactical data system devices that will eventually require IP addresses, so each battery was given its own subnet.

9. Light Antiaircraft Missile (LAAM) Battalion

There is currently only one LAAM battalion in the Marine Corps. Nonetheless, each Marine Air Wing was provided an address to use for the LAAM battalion if it should be reactivated. The allocation of the LAAM class C network number is very similar to that of the LAAD battalion.

F. COMBAT SERVICE SUPPORT ELEMENT (CSSE)

1. Force Service Support Group (FSSG) Headquarters

The FSSG establishes a Combat Service Support Operations Center (CSSOC) as its tactical "command post." The FSSG itself is highly task-organized and it is difficult to know exactly how it will be employed on a given operation. The FSSG will employ a TDN Gateway to internetwork its many battalions and Combat Service Support Elements (CSSEs) and Combat Service Support Detachments (CSSDs). The FSSG Gateway will be addressed in the same way as the Division and Air Wing TDN Gateways. A TDN Server will be fielded to each battalion in the FSSG and four Servers will be fielded to the FSSG HQ. To maintain maximum flexibility of addressing, one classified class C network number and one unclassified class C network number were assigned to each FSSG battalion, the FSSG headquarters (staff), and the CSSOC.

2. FSSG Battalions

Each of the FSSG's battalions will establish a LAN. The Supply Battalion will certainly have both classified and unclassified LANs because it must process and track automated requisitions throught the SASSY Management Unit (SMU). The Medical Battalion will install a network that connects to medical facilities in the U.S. for telemedicine purposes.

UNIT/ORG	NETWORK#	SUBNET#	HOST RANGE	COMMENTS
LAAD Battalion	N.N.110.0	N.N.110.0	N.N.110.1-5	router
		(3 bit subnet)	N.N.110.6	LAN file server
			N.N.110.7	DMS MTA
			N.N.110.8	SNS/NES/INE
			N.N.110.9	DNS server
			N.N.110.10	DHCP server
			N.N.110.11	SMTP mail server
			N.N.110.12	Web server
			N.N.110.13	management workstation
			N.N.110.14-16	UPSs
			N.N.110.17-20	External drives/RAID
			N.N.110.21-24	TCIMs
			N.N.110.25-30	repeaters
			N.N.110.31	subnet broadcast
	3 bit subnet->	N.N.110.32	N.N.110.34	main TCO workstation
			N.N.110.35-62	LAAD Bn LAN users
	3 bit subnets->	N.N.110.64	N.N.110.65-95	LAAD Bn LAN users
LAAD Batteries		N.N.110.96	N.N.110.97-126	LAAD Battery
		N.N.110.128	N.N.110.129-158	LAAD Battery
		N.N.110.160	N.N.110.161-190	LAAD Battery
		N.N.110.192	N.N.110.193-222	LAAD Battery
		N.N.110.224	N.N.110.225-254	LAAD Battery

Table A.23 Example IP address plan for the Low Altitude Air Defense Battalion.

G. SUMMARY

The Tactical Data Network IP address allocation plan presented in this study is consistent with current best practices in the IP internetworking field. It provides enough address space for not only current tactical IP address requirements but also provides room for future growth. With the advent of Internet Protocol version 6 address *space* will become less of a concern, but address hierarchy will continue to be critical to routing efficiency. CIDR is the prototype for next generation hierarchical routing, and OSPFv2 is currently being upgraded to work with IPv6. By employing Classless Inter-Domain Routing (CIDR) and OSPFv2 in TDN, the Marine Corps positions itself to make a smooth transition to the next-generation internetworking environment.

APPENDIX B. ACRONYMS

AAL	ATM Adaptation Layer
AAV	Amphibious Assault Vehicle
AAAV	Advanced Amphibious Assault Vehicle
ACE	Aviation Combat Element
AFFOR	Air Force Forces Commander
AFATDS	Advanced Field Artillery Tactical Data System
API	Application Programming Interface
ARFOR	Army Forces Commander
ATACC	Advanced Tactical Air Command Center
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Network
BGP-4	Border Gateway Protocol version 4
Bn	Battalion
BOOTP	BOOTstrap Protocol
bps	Bits per second
C^2	Command and Control
C4I	Command, Control, Communications, Computers and Intelligence
CDP	Conditioned DiPhase
CD-ROM	Compact Disc Read Only Memory
CE	Command Element
CIDR	Classless Inter-Domain Routing
CLNP	Connectionless Network Protocol
COC	Combat Operations Center
COE	Common Operating Environment
COP	Common Operational Picture
COTS	Commercial Off-The-Shelf
CP	Command Post
CPU	Central Processing Unit
CSS	Communications Support System/Combat Service Support
CSSE	Combat Service Support Element
CTAPS	Contingency Theater Air Control Automated Planning System

DACT	Digital Automated Communications Terminal
DARPA	Defense Advanced Research Projects Agency
DASC	Direct Air Support Center
DCE	Data Communications Equipment
DCP	Distributed Collaborative Planning
DDN	Defense Data Network
DHCP	Dynamic Host Configuration Protocol
DII	Defense Information Infrastructure
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DMS	Defense Messaging System
DNS	Domain Name System
DoD	Department of Defense
DSN	Defense Switched Network
DSNET1	Defense Secure Network 1 (SECRET)
DSNET2	Defense Secure Network 2 (TOP SECRET)
DSNET3	Defense Secure Network 3 (TOP SECRET SCI)
DSVT	Digital Subscriber Voice Terminal
DTE	Data Terminal Equipment
ECU	Environmental Control Unit
ESP	Encapsulating Security Payload
FDC	Fire Direction Center
FDDI	Fiber Distributed Data Interface
FMF	Fleet Marine Force
FSCC	Fire Support Coordination Center
FSSG	Force Service Support Group
FTP	File Transfer Protocol
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCE	Ground Combat Element
GOSIP	Government Open Systems Interconnection Profile
GPS	Global Positioning System

GUI	Graphical User Interface
GW	Tactical Data Network Gateway
HD	Hard Drive
HQ	Headquarters
HTML	HyperText Markup Language
HTTP	HyperText Transport Protocol
IAB	Internet Architecture Board
IANA	Internet Assigned Number Authority
IAS	Intelligence Analysis System
ID	Identifier
IDASC	Improved Direct Air Support Center
IDNX	Integrated Digital Network Exchange
IEEE	Institute of Electrical and Electronics Engineers
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IMTA	Intermediate Message Transfer Agent
INE	Inline Network Encryptor
INRIA	Institut National de Recherche en Informatique et en Automatique
InterNIC	Internet Network Information Center
IP	Internet Protocol
IPng	Internet Protocol Next Generation (also IPv6)
IPngWG	Internet Protocol Next Generation Working Group (IETF)
IPSEC	Internet Protocol Security Architecture
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6 (also IPng)
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISOC	Internet Society
ITSDN	Integrated Tactical-Strategic Data Network
ITU	International Telecommunications Union
JIEO	Joint Interoperability Engineering Organization
JMCIS	Joint Maritime Command Information System
JOTS	Joint Operational Tactical System

JTF	Joint Task Force
JWICS	Joint World-wide Intelligence Communications System
KIV-7	inline encryption device
LAAD	Low Altitude Air Defense
LAAM	Light AntiAircraft Missile
LAN	Local-Area Network
LAP-B	Link Access Protocol B
LAR	Light Armored Reconnaissance
LAV	Light Armored Vehicle
LLC	Logical Link Control
MACG	Marine Air Control Group
MACS	Marine Air Control Squadron
MAG	Marine Air Group
MAGTF	Marine Air-Ground Task Force
MALS	Marine Aviation Logistics Squadron
MARCORSYSCOM	Marine Corps Systems Command
MATCS	Marine Air Traffic Control Squadron
MARFOR	Marine Forces
MARFORLANT	Marine Forces Atlantic
MARFORPAC	Marine Forces Pacific
MAW	Marine Air Wing
MBone	Multicast Backbone
MCCDC	Marine Corps Combat Development Command
MCSSC2	Marine Combat Service Support Command and Control System
MCTSSA	Marine Corps Tactical Systems Support Activity
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MIL-STD	Military Standard
MMT	Multimedia Terminal
MSE	Mobile Subscriber Equipment
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
MTWS	MAGTF Tactical Warfare Simulation

MWCS	Marine Wing Communications Squadron
MWSG	Marine Wing Support Group
MWSS	Marine Wing Support Squadron
NAK	Negative Acknowledgement
NAVFOR	Navy Forces Commander
NCCOSC	Naval Command Control and Ocean Surveillance Center
NCTAMS	Naval Computer and Telecommunications Area Master Station
NES	Network Encryption System (Motorola Inc.)
NIC	Network Information Center/Network Interface Card
NII	National Information Infrastructure
NIPRNET	Non-secure IP Router Network
NPS	Naval Postgraduate School
NRC	National Research Council
ODN	Open Data Network
ORD	Operational Requirements Document
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OSPFv2	Open Shortest Path First Protocol version 2
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PEM	Privacy Enhanced Mail
PEP	Power Entry Panel
POSIX	Portable Operating System Interface for Computer Environments
PPP	Point-to-Point Protocol
QoS	Quality of Service
RAID	Redundant Array of Inexpensive Disks
REGT	Regiment
RFC	Request For Comments
RSVP	Resource Reservation Protocol
SB-3865	30-line portable digital tactical circuit switch
SCI	Special Compartmented Information (TOP SECRET)
SEP	Signal Entry Panel
SINCGARS	Single Channel Ground and Airborne Radio System

SIPP	Simple Internet Protocol Plus
SIPRNET	Secure IP Router Network
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPv2	Simple Network Management Protocol version 2
SNS	Secure Network Server
SQDN	Squadron
SRIG	Surveillance, Reconnaissance and Intelligence Group
STD	Standard (Internet Standard)
STEP	Standardized Tactical Entry Point
TACC	Tactical Air Command Center
TADILS	Tactical Data Links
TADIX	Tactical Data Information Exchange System
TASDAC	Tactical Secure Data Communications
TCIM	Tactical Communications Interface Module
TCO	Tactical Combat Operations
TCP	Transmission Control Protocol
TDC	Theater Deployable Communications
TDN	Tactical Data Network
TDS	Tactical Data System
TELNET	Virtual terminal protocol in TCP/IP protocol suite
TNS	Tactical Name Server
TPN	Tactical Packet Network
TSQ-184	Analog Technical Control System
TSQ-188	Digital Technical Control System
TTC-42	150-line capacity digital tactical circuit switch system
TTL	Time-To-Live
TS3	TOP SECRET Support System
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UPS	Uninterruptable Power Supply
USMC	United States Marine Corps

VTC	Videoteleconference
WAN	Wide-Area Network
WLA	Wireline Adapter
WWW	World Wide Web
X.25	ISO packet-switching protocol standard
X.400	ISO electronic mail protocol standard used in DMS
X.500	ISO network directory services protocol standard used in DMS
XTP	Xpress Transport Protocol
VINES	Virtual Network System (Banyan Inc.)

APPENDIX C. ON-LINE AVAILABILITY

This thesis is available on the World-Wide Web. The HyperText Markup Language (HTML) version can be found at

http://www.stl.nps.navy.mil/~jenierle/thesis.html

and can be viewed on-line using a Web browser such as *Netscape Navigator* [NCC,96]. For ease of downloading and printing, a *PostScript* version of this thesis is available at

http://www.stl.nps.navy.mil/~jenierle/PostScript.html

When downloaded, these *PostScript* files may be printed directly to any *PostScript*-compatible printing device or viewed on a terminal with a *PostScript* document viewer. Instructions on how to obtain and use *PostScript* viewers are available at

http://www.math.washington.edu/~kaupe/teaching/307_spring96/PostScript.html

In order to reduce download time, some of these thesis *PostScript* files have been compressed. Most Web browsers are (or can be) configured to automatically decompress files once downloaded. If your browser cannot access the appropriate decompression utility, you will have to save the downloaded binary files to disk and decompress them off-line before printing or viewing.

The Information Infrastructure Research Group (IIRG) at the Naval Postgraduate School maintains a Web page [IIRG,96] that has a link to this thesis and to other completed and in-progress work by IIRG group members. The IIRG Web page is available at ***http://www.stl.nps.navy.mil/~iirg***.

Questions regarding on-line access to this thesis should be directed to the Information Infrastructure Research Group at *iirg@stl.nps.navy.mil* or to Don Brutzman at *brutzman@cs.nps.navy.mil* or (408)-656-2149.

REFERENCES

Adamson, R., "Internetworking the Navy," *IPng: Internet Protocol Next Generation*, Addison-Wesley, Reading Massachusetts, 1996.

Armitrage, Grenville, *IPv6 and Neighbor Discovery over ATM*, work in progress, Internet Engineering Task Force (IETF), 29 April 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipatm-ipv6nd-02.txt*

Atkinson, R., *Security Architecture for the Internet Protocol*, Request for Comments 1825, Internet Engineering Task Force (IETF), August 1995. Available at *ftp://ds.internic.net/rfc/rfc1825.txt*

Baker, Steven, "The Future of Major Protocols," *UNIX REVIEW*, vol. 12 no. 5, pp. 23-29, May 1994.

Bigelow,R., *Internetworking: Planning and Implementing a Wide-Area Network for K-12 Schools,* Masters Thesis, Naval Postgraduate School, Monterey California, September 1995. Available at *http://www.stl.nps.navy.mil/~rjbigelo/thesis.html*

Borden, M., Crawley,E., Davis, B. and Batsell, S., *Integration of Real-Time Services in an IP-ATM Network Architecture*, Request for Comments 1821, Internet Engineering Task Force (IETF), August 1995. Available at *ftp://ds.internic.net/rfc/rfc1821.txt*

Bound, J., "Implementing IPng on a BSD Host," *IPng: Internet Protocol Next Generation*, Addison-Wesley, Reading Massachusetts, 1996.

Braden, R., Clark, D. and Shenker, S., *Integrated Services in the Internet Architecture: an Overview*, Request for Comments 1633, Internet Engineering Task Force (IETF), June 1994. Available at *ftp://ds.internic.net/rfc/rfc1633.txt*

Braden, R., Zhang, L., Berson, S., Herzog, S. and Jamin, S., *Resource Reservation Protocol (RSVP) Functional Specification*, work in progress, Internet Engineering Task Force (IETF), 18 March 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-rsvp-spec-11.txt*

Bradner, Scott O. and Mankin, Allison, editors, *IPng: Internet Protocol Next Generation*, Addison-Wesley, Reading Massachusetts, 1996.

Bradner, Scott O., *The Internet Standards Process Revision 3*, work in progress, Internet Engineering Task Force (IETF), April 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-poised95-std-proc-3-06.txt*

Braudes, R. and Zabele, S., *Requirements for Multicast Protocols*, Request for Comments 1458, Internet Engineering Task Force (IETF), May 1993. Available at *ftp://ds.internic.net/rfc/rfc1458.txt*

Bruno, L., " Internet Security: How Much Is Enough?," *DATA COMMUNICATIONS*, vol. 25 no. 5, April 1996.

Brutzman, Donald P. and Reimers, Stephen, "Internet Protocol over Seawater (IP/SW): Towards Interoperable Underwater Networks," Unmanned Untethered Submersibles Technology 95, Northeastern University, Nahant Massachusetts, pp. 444-457, September 25-27 1995. Available at *ftp://taurus.cs.nps.navy.mil/pub/auv/ipoversw.ps*

Brutzman, Donald P., "Graphics Internetworking: Bottlenecks and Breakthroughs," *Digital Illusions*, Clark Dodworth editor, Addison-Wesley, Reading Massachusetts, 1996. Available at *http://www.stl.nps.navy.mil/~brutzman/vrml/breakthroughs.html*

Buddenberg, R., *Computer Networking and C3I Systems for Emergency Services*, Naval Postgraduate School, 1995. Available at *http://dubhe.cc.nps.navy.mil/~budden/book/table_contents.html*

Carl-Mitchell, Smoot, "The New Internet Protocol," *UNIX REVIEW*, vol. 13 no. 7, pp. 31-38, June 1995.

Cerf, V., *The Internet Activities Board*, Request for Comments 1160, Internet Engineering Task Force (IETF), May 1990. Available at *ftp://ds.internic.net/rfc/rfc1160.txt*

Chmielewski, B., Advanced Field Artillery Tactical Data System (AFATDS) Project Officer, Headquarters U.S. Marine Corps, interview, 28 March 1996.

Cisco Systems Inc., *Increasing Security on IP Networks*, technical tips Web page, San Jose California, 1995. Available at *http://www.cisco.com/warp/public/701/31.html*

Cisco Systems Inc., *Designing Large-Scale IP Internetworks*, informational brochure, San Jose California, 1995. Additional information available at *http://www.cisco.com*

Comer, Douglas E., *Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture*, third edition, Prentice Hall, Englewood Cliffs New Jersey, 1995.

Commandants Warfighting Laboratory (WARLAB), *Technology Exploration and Exploitation Plan*, United States Marine Corps, Quantico Virginia, 1995. Available at *http://138.156.204.100/www/cwl/planch1.htm*

Cortese, A., "Here Comes the Intranet," *BUSINESSWEEK*, pp. 76-85, 26 February 1996.

Cummiskey, J., *Interoperability of Palmtop Computers with the U.S. Marine Corps Data Automated Communications Terminal (DACT) to Rapidly Disseminate Combat Order Message Packets Over Wired and Wireless Channels*, Masters thesis, Naval Postgraduate School, September 1996. Available at *http://www.stl.nps.navy.mil/~jccummis*

Deering, S., *Host Extensions for IP Multicasting*, Request for Comments 1112, Internet Engineering Task Force (IETF), August 1989. Available at *ftp://ds.internic.net/rfc/rfc1112.txt*

Deering, S. and Hinden, R., *Internet Protocol, Version 6 (IPv6) Specification*, Request for Comments 1883, Internet Engineering Task Force (IETF), December 1995. Available at *ftp://ds.internic.net/rfc/rfc1883.txt*

Defense Information Systems Agency (DISA), *Defense Information Infrastructure Master Plan: Executive Summary,* Web page, Washington DC, 28 July 1995. Available at *http://www.disa.mil/dii/diiexe/execsum1.html*

Defense Information Systems Agency (DISA), *Defense Information Systems Network (DISN) Strategy,* Web page, Washington DC, July 1995. Available at *http://www.disa.mil/disn/disnhome.html*

Defense Information Systems Agency (DISA), *Global Command and Control System (GCCS)*, Web page, 1996. Available at *http://164.117.208.50/newgoal.html*

Defense Information Systems Agency (DISA), *Department of Defense (DoD) Network Information Center (NIC)*, Web page, 1996. Available at *http://nic.ddn.mil*

DeLoria, Wayne, "DMS: The Journey from Here to the Desktop," *CHIPS*, Naval Computer and Telecommunications Area Master Station LANT, pp. 10-19, January 1996. Available at *http://www.chips.navy.mil/chips/archives/96_jan/contents.htm*

Department of the Army, *Department of the Army C4I Technical Architecture version 3.1*, 31 March 1995. Available at *http://www.seas.gwu.edu/seas/fa53/ta/techarch.html*

Droms, R., *Dynamic Host Configuration Protocol,* Request for Comments 15 41, Internet Engineering Task Force (IETF), October 1993. Available at *ftp://ds.internic.net/rfc/rfc1541.txt*

Droms, R., *Dynamic Host Configuration Working Group*, Web page, Internet Engineering Task Force, 1996. Available at *http://www.ietf.cnri.reston.va.us/html.charters/dhc-charter.html*

Eastlake, D. and Kaufman, C., *Domain Name System Security Extensions*, work in progress, Internet Engineering Task Force (IETF), 30 January 1996. Available at *ftp://ftp.ietf.cnri.reston.va.us/internet-drafts /draft-ietf-dnssec-secext-09.txt*

Emswiler, Tracey, *Internetworking: Using the Multicast Backbone (MBone) for Distance Learning*, Masters Thesis, Naval Postgraduate School, Monterey California, September 1995. Summary video available at *http://www.stl.nps.navy.mil/~iirg/emswiler/emswiler.qt.Z*

Fleischman, E., "IPng and Corporate Resistance to Change," *IPng: Internet Protocol Next Generation*, Addison-Wesley, Reading Massachusetts, 1996.

Floyd, S., Jacobson, V., Liu, C., McCanne, S. and Zhang, L, *A Reliable Multicast Framework for Light-weight Sessions and Application Level Framing,* ACM SIGCOMM 95, pp. 342-356, August 1995. Available at *ftp://ftp.ee.lbl.gov/papers/link.ps.Z*

Fuller, V., Li, T., Yu, J. and Varadhan, K., *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*, Request for Comments 1519, Internet Engineering Task Force (IETF), September 1993. Available at *ftp://ds.internic.net/rfc/rfc1519.txt*

Galvin, P. and McCloghrie, *Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*, Request for Comments 1446, Internet Engineering Task Force (IETF), 3 May1993. Available at *ftp://ds.internic.net/rfc/rfc1446.txt*

Gaunter, C., Captain U.S. Marine Corps, Banyan Worldwide Support Officer, Marine Corps Systems Command-East, telephone interview, Quantico Virginia, 10 April 1996.

Ghosh, S., "Defining the Key Issues in Mobile TCP/IP Networking," *TELECOMMUNICATIONS*, vol. 27 no. 12, pp. 37-42, December 1993.

Gilligan, R. and Nordmark, E., *Transition Mechanisms for IPv6 Hosts and Routers*, Request for Comments 1933, Internet Engineering Task Force (IETF), April 1996. Available at *ftp://ds.internic.net/rfc/rfc1933.txt*

Grehan, P., "IPv6 Implementation," electronic mail message, Ipsilon Networks Inc., Palo Alto California, 10 April 1996.

Handley, M. and Jacobson, V., *SDP: Session Description Protocol*, work in progress, Internet Engineering Task Force (IETF), 22 November 1995. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mmusic-sdp-01.txt*

Henderson, Scott, "Deployment of Network Systems Security Products within the DoN to Support DMS," *CHIPS*, Naval Computer and Telecommunications Area Master Station LANT, pg. 26, January 1996. Available at *http://www.chips.navy.mil/chips/archives/96_jan/contents.htm*

Hinden, Robert., *IP Next Generation Overview*, Web page, 14 May 1995. Available at *http://playground.sun.com/pub/ipng/html/INET-IPng-Paper.html*

Hinden, R., *IP version 6 Addressing Architecture*, Request for Comments 1884, Internet Engineering Task Force (IETF), December 1995. Available at *ftp://ds.internic.net/rfc/rfc1884.txt*

Hinden, R., *IP Next Generation*, Web page, 1996. Available at *http://playground.sun.com/pub/ipng/htmlipng-main.html*

Hovey, R. and Bradner, S., *The Organizations Involved in the Internet Standards Process*, work in progress, Internet Engineering Task Force (IETF), April 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-poised95-ietf-org-01.txt*

Hughes, Kevin, "Entering the World Wide Web: A Guide to Cyberspace," Enterprise Integration Technologies, Palo Alto California, 1994. Available at *http://www.eit.com/web/www.guide/*

Imielinski, T. and Navas, J., *GPS-Based Addressing and Routing*, work in progress, Internet Engineering Task Force (IETF), 8 March 1996. Available at *ftp://ds.internic.net/internet-drafts/draft-rfced-exp-navas-00.txt*

Information Infrastructure Research Group (IIRG), Web page, Naval Postgraduate School, Monterey California, 1996. Available at *http://www.stl.nps.navy.mil/~iirg*

Internet Engineering Task Force (IETF) Secretariat, *IPng Working Group Charter*, Web page, 1996. Available at *http://ietf.cnri.reston.va.us/html.charters/ipngwg-charter.html*

Internet Network Information Center (InterNIC), *InterNIC*, Web page, Herndon Virginia, 1996. Available at *http://rs.internic.net*

Ipsilon Networks Inc., *IP Switching: The Intelligence of Routing, the Performance of Switching*, Ipsilon technical white paper, February 1996. Available at *http://www.ipsilon.com/productinfo/techwp1.html*

Jacobson, V., *Multimedia Conferencing on the Internet,* tutorial presented at 1994 SIGCOMM Conference (SIGCOMM '94), University College London, London, 30 August 1994.

Jeffries, Ron, "Three Roads to Quality of Service: ATM, RSVP, and CIF," *TELECOMMUNICATIONS*, vol. 30 no. 4, pg. 77, April 1996.

Joint Interoperability Engineering Organization (JIEO), *Joint Task Force Tactical Communications Architecture*, JIEO Report 8125, March 1995.

Joint Interoperability Engineering Organization (JIEO), *Integrated Tactical Strategic Data Networking (ITSDN) "Quick Fix" Engineering Plan,* inter-agency coordination draft, 25 June 1995.

Joint Staff, *C4I for the Warrior*, Washington DC, 12 June 1993.

Knight, J., Multicast Transport Protocols, Web page, Loughborough University of Technology, Leicestershire United Kingdom, 1996. Available at *http://hill.lut.ac.uk/DS-Archive/MTP.html*

Kumar, V., *MBone: Interactive Multimedia on the Internet*, New Riders Publishing, Indianapolis Indiana, 1996.

Kumar, V., *The MBone Information Web*, Web page, 1996. Available at *http://www.best.com/~prince/techinfo/MBone.html*

Lotus Development Corporation, *www.lotus.com*, Web page, 1996. Available at *http://www.lotus.com*

Macedonia, Michael R. and Brutzman, Donald P., "MBone Provides Audio and Video Across the Internet," *IEEE COMPUTER*, vol. 27 no. 4, April 1994, pp. 30-36. Available at *ftp://taurus.cs.nps.navy.mil/pub/13la/mbone.html.*

Macedonia, Michael R., *A Network Software Architecture for Large Scale Virtual Environments*, Ph.D. Dissertation, Naval Postgraduate School, Monterey California, June 1995. Available at *http://www.cs.nps.navy.mil/research/npsnet/publications/Michael.Macedonia.thesis.ps.Z*

Marine Corps Combat Development Command (MCCDC), *Operational Requirements Document (ORD) for the Tactical Data Network (TDN)*, Quantico Virginia, July 1995.

Marine Corps Combat Development Command (MCCDC), *United States Marine Corps Technical Architecture version 1.0*, Quantico Virginia, 5 October 1995.

Marine Corps Systems Command (MARCORSYSCOM), *MAGTF C4I Transition to the Global Command and Control System (GCCS) Common Operating Environment,* Quantico Virginia, 15 March 1994.

Marine Corps Systems Command (MARCORSYSCOM), *Tactical Data Network System Description,* Quantico Virginia, September 1995.

Marine Corps Systems Command (MARCORSYSCOM), *Tactical Data Network (TDN) Server Specification,* Quantico Virginia, 16 October 1995.

Marine Corps Systems Command (MARCORSYSCOM), *Tactical Data Network (TDN) Gateway Performance Specification,* Quantico Virginia, 16 October 1995.

Marine Corps Tactical Systems Support Activity (MCTSSA), *Tactical Combat Operations (TCO): Fielding Plan*, Camp Pendleton California, 1995.

Marine Corps Tactical Systems Support Activity (MCTSSA), *Advance Tactical Air Command Central (ATACC),* Web page, Camp Pendleton California, 1996. Available at *http://mctssa-gw.usmc.mil/projects.html*

McCann, J., Deering, S. and Mogul, J., *Path MTU Discovery for IP version 6,* work in progress, Internet Engineering Task Force (IETF), 22 April 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipngwg-pmtuv6-02.txt*

McNealis, Martin, "IPv6 Implementation," electronic mail message, Cisco Systems Inc., San Jose California, 10 April 1996.

Medlin, B., "IPv6 Host Implementation," electonic mail message, Hewlett-Packard Inc., Cupertino California, 16 April 1996.

Morales, J., *Tactical DMS: A Global Broadcast Service Option*, Masters Thesis, Naval Postgraduate School, Monterey California, June 1996.

Moy, J., *OSPF Version 2*, Request for Comments 1583, Internet Engineering Task Force (IETF), March 1994. Available at *ftp://ds.internic.net/rfc/rfc1583.txt*

Murai, J., Nakamura, O., Tominaga, A. and Teraoka, F., *Problems and Solutions of DHCP: Experiences with DHCP Implementation and Operation*, WIDE Project online report, 28 April 1995. Available at *http://info.isoc.org/HMP/PAPER/127/html/paper.html*

National Research Council, NRENAISSANCE Committee, *Realizing the Information Future: the Internet and Beyond*, National Academy Press, Washington DC, 1994. Available at *http://www.nap.edu/nap/online/rtif/*

National Research Council, NII 2000 Steering Committee, *The Unpredictable Certainty: Information Infrastructure through 2000*, National Academy Press, Washington DC, 1996. Available at *http://www.nap.edu/nap/online/unpredictable/*

Naval Command, Control and Ocean Surveillance Center (NCCOSC), *IP Addressing Study (IPADD)*, San Diego California, 1995.

Netscape Communications Corporation (NCC), *Download Netscape Navigator Software*, Web page, Mountain View California, 1996. Available at *http://www.netscape.com/comprod/mirror/client_download.html* also available at *ftp2.netscape.com*

Partridge, C., Mendez, T. and Milliken, W., *Host Anycasting Service*, Request for Comments 1546, Internet Engineering Task Force (IETF), November 1993. Available at *ftp://ds.internic.net/rfc/rfc1546.txt*

Passmore, David, "Next Generation IP: Construction Ahead", *BUSINESS COMMUNICATIONS REVIEW*, pp. 18-20, March 1995.

Perkins, C. and Johnson, D., *Mobility Support in IPv6,* work in progress, Internet Engineering Task Force (IETF), January 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-ipv6-00.txt*

Perkins, C., editor, *IP Mobility Support*, work in progress, Internet Engineering Task Force (IETF), February 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-mobileip-protocol-16.txt*

Postel, J., editor, *Internet Official Protocol Standards*, Standard 1 (STD-1), Internet Architecture Board, March 1996. Available at *ftp://venera.isi.edu/in-notes/std/std1.txt*

Rekhter, Y. and Li, T., *A Border Gateway Protocol (BGP-4)*, Request for Comments 1654, Internet Engineering Task Force (IETF), 21 July 1994. Available at *ftp://ds.internic.net/rfc/rfc1654.txt*

Rekhter, Y. and Li, T., *An Architecture for IPv6 Unicast Address Allocation*, Request for Comments 1887, Internet Engineering Task Force (IETF), December 1995. Available at *ftp://ds.internic.net/rfc/rfc1887.txt*

Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G. and Lear, E., *Address Allocation for Private Internets*, Request for Comments 1918, Internet Engineering Task Force (IETF), February 1996. Available at *ftp://ds.internic.net/rfc/rfc1918.txt*

Rekhter, Y., Lothberg, P., Hinden, R., Deering, S. and Postel, J., editors, *An IPv6 Provider-Based Unicast Address Format*, work in progress, Internet Engineering Task Force (IETF), March 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-ipngwg-unicast-addr-fmt-04.txt*

Reitzel, Andrea, editor, "Internet Engineering Task Force December 1995 Meeting Report," Mitre Corporation, January 1996.

Rescoria, E. and Schiffman, A., *The Secure Hypertext Transfer Protocol*, work in progress, Internet Engineering Task Force (IETF), February 1996. Available at *ftp://ftp.ietf.cnri.reston.va.us /internet-drafts/ draft-ietf-wts-shttp-01.txt*

Rogers, Amy, "Ready for the 'Net?,"*COMMUNICATIONS WEEK*, 4 March 1996.

Russell, D. and Gangemi, G., *Computer Security Basics*, O'Reilly and Associates, Sebastopol California, 1991.

Sawyers, W., *Performance Testing for the Marine Air Ground Task Force Tactical Warfare Simulation,* Masters Thesis, Naval Postgraduate School, Monterey California, September 1995.

Spector, A., "Army Tactical Name Server," electronic mail message, SAIC, San Diego California, 12 April 1996.

Starburst Communications Inc., *Starburst MFTP™ Compared to Today's File Transfer Protocols*, white paper, Concord Massachussetts, 1996. Available at *http://www.starburstcom.com/white.htm*

Symington, S., Wood, D. and Pullen, J., "Use of IPng in Combat Simulation," *IPng: Internet Protocol Next Generation*, Addison-Wesley, Reading Massachusetts, 1996.

Tallerico, D. and Reitzel, A., *The Next Generation Internet Protocol*, Mitre Inc., 28 September 1995.

Thomson, Susan and Narten, Thomas, *IPv6 Stateless Address Autoconfiguration*, work in progress, Internet Engineering Task Force (IETF), December 1995. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-addrconf-ipv6-auto-07.txt*

Tiddy, M., *Internetworking: Economic Storage and Retrieval of Digital Audio and Video for Distance Learning*, Masters Thesis, Naval Postgraduate School, September 1996. Available at *http://www.stl.nps.navy.mil/~metiddy/thesis.html*

Trepanier, D., *Internetworking: Recommendations on Network Management for K-12 Schools*, Masters Thesis, Naval Postgraduate School, September 1995.

Trinity College, *IPng: Internet Protocol Next Generation*, Web page, Dublin Ireland, 1995. Available at *http://ganges.cs.tcd.ie/4ba2/ipng/index.html*

United States Army, *Force XXI*, Web page, 1996. Available at *http://140.139.18.189:1100/force21/f21hoome.html*

Vixie, P., Rekhter, Y., Bound, J. and Thomson, S., *Dynamic Updates in the Domain Name System*, work in progress, Internet Engineering Task Force (IETF), 14 March 1996. Available at *ftp://ietf.cnri.reston.va.us/internet-drafts/draft-ietf-dnsind-dynDNS-09.txt*

Voigt,R., *A Hierarchical Approach to Multicast in a Datagram Internetwork*, PhD Dissertation, Naval Postgraduate School, Monterey California, March 1996. Available at *ftp://ftp.nps.navy.mil/pub/ece/rjvoigt/charm.ps.z*

Walker, Richer, & Quinn (WRQ), *IP Addressing*, technical support Web page, 1995. Available at *http://www.wrq.com*

Waters, G., *User-Based Security Model for SNMPv2*, Request for Comments 1910, Internet Engineering Task Force (IETF), 28 February 1996. Available at *ftp://ds.internic.net/rfc/rfc1910.txt*

Weaver, Alfred, *What is the Xpress Transport Protocol?*, information paper, Network Xpress Inc., Charlottesville Virginia, 1994. Available at *http://www.cs.virginia.edu/~netlab/xtp_stuff/what_is_xtp.ps* (postscript file)

Wobus, John, *DHCP FAQ*, frequently asked questions Web page, 12 April 1996. Available at *http://web.syr.edu/~jmwobus/comfaqs/dhcp.faq.html*

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center 8725 John J. Kingman Rd, STE 0944 Ft. Belvoir, Virginia 22060-6218	2
2.	Dudley Knox Library Naval Postgraduate School 411 Dyer Rd. Monterey, California 93943-5101	2
3.	Director, Training and Education MCCDC, Code C46 1019 Elliot Road Quantico, Virginia 22134-5027	1
4.	Director, Marine Corps Research Center MCCDC, Code C40RC 2040 Broadway Street Quantico, Virginia 22134-5107	1
5.	Director, Studies and Analysis Division MCCDC, Code C45 3300 Russell Road Quantico, Virginia 22134-5130	1
6.	Commandant of the Marine Corps C4I Directorate, Code CS Washington, DC 20380-0001	1
7.	Commanding General, Marine Corps Systems Command Attn: CAPT D. Beutel USMC, TDN Project Officer C4I/COMM-S 2033 Barnett Ave. Suite 315 Quantico, Virginia 22134-5080	2
8.	Commanding Officer,Marine Corps Tactical Systems Support Activity Attn: CAPT D. Wells USMC, TDN Project Officer Communications Systems Division Camp Pendleton, California 92055-5000	1

9. Defense Modeling and Simulation Office 1
1901 N. Beauregard St., Suite 510
Alexandria, Virginia 22311

10. Professor Dan C. Boger, Code CC 1
Naval Postgraduate School
Monterey, California 93943

11. Assistant Professor Don Brutzman, Code UW/Br 2
Naval Postgraduate School
Monterey, California 93943

12. Rex Buddenberg, Code SM/Bu 1
Naval Postgraduate School
Monterey, California 93943

13. Erik Chaum 1
Naval Undersea Warfare Center
Code 2251, BLDG 1171-3
1176 Howell St.
Newport, Rhode Island 02841-1708

14. Keith Davis 1
SPAWAR
2 Littlebrook Circle
Fredricksburg, Virginia 22405

15. Cynthia Martin 1
Defense Information Systems Agency
10701 Parkridge Blvd.
Reston, Virginia 22091

16. Major Theresa Orihuela USA 1
ITSDN Program Manager
DISA Westhem, WE3351
11440 Isaac Newton Square
Reston, Virginia 22090-5087

17. Captain James E. Nierle USMC 2
Joint Interoperability Test Command
Fort Huachuca, Arizona 85613-7020